NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FIGHTING NETWORKS: THE DEFINING CHALLENGE OF IRREGULAR WARFARE

by

Arleigh William Dean

June 2011

Thesis Co-Advisors: John Arquilla
Michael Freeman

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Fighting Networks: The Defining Challenge of Irregular Warfare		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Arleigh William Dean			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number N/A			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

This study examines how networks fight, and how to counter networks. Networks, empowered by information technology, play a powerful role in many different aspects of social and organizational interaction. Notably, recent confrontations with networked opponents have strained the U.S. military, and produced time-intensive, brutally complex, and costly irregular warfare in Iraq and Afghanistan. The challenges that these fighting networks present require a close examination of how they fight, and most importantly, how to combat the threat they pose.

The primary purpose of this study is to examine the role of networks in irregular warfare, where they are central and prevalent. Regardless of its many forms, the most salient aspect of modern irregular warfare is the increasingly networked nature of the antagonists. Countering these opponents requires a detailed understanding of the organization, doctrine, methods, and information usage, which both empower networks and generate vulnerabilities.

This research generated a theoretical framework that draws on the rich bodies of knowledge that inform network theory, network-based operations, irregular warfare, organizational theory, and information strategy. Each of these theoretical areas provided hypotheses for identifying causal factors, which led to an understanding of how networks fight, and development of a systematic framework for countering them.

Comparative case studies focused on a cluster of networks engaged in irregular warfare, which served to test this framework. This cluster consists of three cases, each marked by "tough opponents," and network-based organizations operating in the information age: the Chechen separatists, Lebanese Hezbollah, and Al-Qaeda in Iraq. Overall, this thesis advances theory in a way that provides a systematic understanding of how to counter networked opponents, while generating additional perspective about irregular warfare.

14. SUBJECT TERMS Network Theory, Network-Style Warfare, Netwar, Dark Networks, Organizational Theory, Irregular Warfare, Guerrilla Warfare, Counter-Terrorism (CT), Counter-Insurgency (COIN), Unconventional Warfare (UW), Hybrid Warfare, Asymmetric Warfare, Fusion, Swarming, Information Strategy, Intelligence			**15. NUMBER OF PAGES** 373
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

FIGHTING NETWORKS: THE DEFINING CHALLENGE OF IRREGULAR WARFARE

Arleigh William Dean
Major, United States Army
B.S., United States Military Academy, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
June 2011

Author: Arleigh William Dean

Approved by: Dr. John Arquilla
Thesis Co-Advisor

Dr. Michael Freeman
Thesis Co-Advisor

Dr. Gordon McCormick
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This study examines how networks fight, and how to counter networks. Networks, empowered by information technology, play a powerful role in many different aspects of social and organizational interaction. Notably, recent confrontations with networked opponents have strained the U.S. military, and produced time-intensive, brutally complex, and costly irregular warfare in Iraq and Afghanistan. The challenges that these fighting networks present require a close examination of how they fight, and most importantly, how to combat the threat they pose.

The primary purpose of this study is to examine the role of networks in irregular warfare, where they are central and prevalent. Regardless of its many forms, the most salient aspect of modern irregular warfare is the increasingly networked nature of the antagonists. Countering these opponents requires a detailed understanding of the organization, doctrine, methods, and information usage, which both empower networks and generate vulnerabilities.

This research generated a theoretical framework that draws on the rich bodies of knowledge that inform network theory, network-based operations, irregular warfare, organizational theory, and information strategy. Each of these theoretical areas provided hypotheses for identifying causal factors, which led to an understanding of how networks fight, and development of a systematic framework for countering them.

Comparative case studies focused on a cluster of networks engaged in irregular warfare, which served to test this framework. This cluster consists of three cases, each marked by "tough opponents," and network-based organizations operating in the information age: the Chechen separatists, Lebanese Hezbollah, and Al-Qaeda in Iraq. Overall, this thesis advances theory in a way that provides a systematic understanding of how to counter networked opponents, while generating additional perspective about irregular warfare.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

1/1 AD	1st Brigade, 1st Armor Division
4GW	4th Generation Warfare
ACR	Armored Calvary Regiment
AI	*Ansar al-Islam*
APCs	Armored Personnel Carriers
AQAP	al-Qaeda in the Arabian Peninsula
AQI	al-Qaeda in Iraq
ASC	Anbar Salvation Council
ATGM	Anti-Tank Guided Missile
BCT	Brigade Combat Team
C2	Command and Control
C2W	Command-and-Control Warfare
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
ChRI	Chechen Republic of Ichkerija
CIA	Central Intelligence Agency
COIN	Counter-Insurgency
CT	Counter-Terrorism
EBO	Effects-Based Operations
EIW	Economic Information Warfare
ERV	Euphrates River Valley
EW	Electronic Warfare
F3EA	Find, Fix, Finish, Exploit, Analyze
FID	Foreign Internal Defense
FMI	Field Manual Interim
FOBs	Forward Operating Bases
FOSh	Federal Operational Staff
FRE	Foreign Regime Elements
FSB	Federal Security Services
FSK	*Federalnaya Sluzhba Kontrrazvedki*, Federal Counterintelligence Service of Russia
GrOU	Operational Control Group
GRU	Russian Military Intelligence

HUMINT	Human Intelligence
HVIs	High-Value Individuals
HVTs	High-Value Targets
IAF	Israeli Air Force
IAG	Iraqi Assistance Group
IAI	Islamic Army of Iraq
IBW	Intelligence-based Warfare
IDF	Israel Defense Forces
IE	Information Engagement
IED	Improvised Explosive Device
IO	Information Operations
IRGC	Iranian Revolutionary Guards Corps
ISF	Iraqi Security Forces
ISI	Islamic State of Iraq
ISR	Intelligence, Surveillance, and Reconnaissance
ISR/HUMINT/SIGINT	Intelligence, Surveillance, and Reconnaissance/Human Intelligence/Signals Intelligence
JSOTF	Joint Special Operations Task Force
JSS	Joint Security Stations
MNC-I	Multi-National Corps-Iraq
MND-B	Multi-National Division-Baghdad
MNF	Multi-National Force
MNF-I	Multi-National Forces-Iraq
MNSTC-I	Multi-National Security Transition Command-Iraq
MoD	Ministry of Defense
MSC	Mujahedin Shura Council
MSR	Main Supply Route
MVD	Ministry of Internal Affairs
NAK	National Anti-Terrorist Committee
NCW	Network-Centric Warfare
NGO	Nongovernmental Organization
OGV	Unified Grouping of Federal Forces
OIF	Operation Iraqi Freedom
PLO	Palestinian Liberation Organization
RPG	Rocket-Propelled Grenade

SF	Special Forces
SIGACTS	Significant Actions
SLA	South Lebanese Army
SOD	Systemic Operational Design
SOF	Special Operations Forces
SOI	Sons of Iraq
SRV	Russian Foreign Intelligence Service
SVBIED	Suicide-Vehicle-Born Improvised Explosive Devices
TQJBR or QJBR	*Tanzim al-Qaeda al-Jihadi fi Bilad al-Rafidayn,* Al Qaeda Organization in the Land of the Two Rivers
TRV	Tigris River Valley
TTPs	Tactics, Techniques, and Procedures
U.S.	United States
UAVs	Unmanned Aerial Vehicles
UK	United Kingdom
UN	United Nations
UNSC	United Nations Security Council
UNSCOM	UN Special Commission on Iraq
UW	Unconventional Warfare
VBIED	Vehicle-Borne IED
VNSAs	Violent Non-State Actors
WMD	Weapons of Mass Destruction
WWI	World War I
WWII	World War II

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Much of the inspiration and motivation for this study was provided by operators like Bob Horrigan and Mike McNulty, who led the way in a violent war against rogue networks and provided an example of excellence for countless others to follow. Their example is emulated by operators and analysts actively involved in the fight against networks. These unnamed individuals will never receive enough thanks, but I trust these words further their efforts.

Special thanks to Professors John Arquilla and Michael Freeman whose advice, counsel, and dedicated effort greatly enhanced this study. In addition, other faculty members at the Naval Postgraduate School, including Dorothy Denning, Sean Everton, Gordon McCormick, Kalev Sepp and Hy Rothstein, all provided advice and insights instrumental to making this project what it is.

Much of the operational insights in this paper are due to input and discussions with those intimately involved in countering networks over the last 10 years. In particular, I would like to thank Jeff T., John K., Sam D., Mike W., Guy L., and Josh T.—all fellow students of warfare. As the proverb states, “as iron sharpens iron, so one man sharpens another.”

Most importantly, my utmost gratitude and thanks to Ruth and Hailey, whose unfailing love motivates a husband and father dedicated to protecting them, and who tolerate his obsession with ensuring that this “long war” is as short as possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

This thesis is a study about irregular conflict, and particularly about the qualities that allow modern, violent fighting networks to challenge nation-states. The oft-quoted statement, "it takes a network to fight a network," prompted this research.[1] While this statement appeals to a form of common sense, it is also a significant proposition with serious implications. If it does truly take a network to fight and defeat another network, then this requires considerable organizational re-evaluation, as well as innovation in areas such as doctrine, communications systems, and information strategy.

Examining this proposition requires initially answering the basic question—how do networks fight? The details behind this answer provide significant insight into not only how networks fight, but also what they are; as well the opportunity to explore the nature of modern irregular warfare. It appears that if a network is simply an organizational type, then not much significance exists behind the proposition. However, using their organizational typology, modern fighting networks advance doctrine, promote tactical innovation, and shape information strategy to achieve near-parity in multiple aspects of conflict. Networks are empowered by information technology, but are not always reliant on its use, highlighting the importance of the other factors.

Countering such networks may require similar innovation and the ability to adapt to dramatic changes. The clearest aspect of this change is the dramatic increase in the role of information in irregular warfare. This increasing importance favors networks, which

[1] Stanley A. McChrystal, "It Takes a Network: The New Frontline of Modern Warfare," *Foreign Policy*, March/April 2011, http://www.foreignpolicy.com/articles/2011/02/22/it_takes_a_network; Greg Grant, "The Man Behind Irregular Warfare Push: Mike Vickers," April 7, 2009, http://www.dodbuzz.com/2009/04/07/the-man-behind-irregular-warfare-push-mike-vickers; "It Takes a Network," Meeting of the International Counter-Terrorism Academic Community, ICT Newsletter, Spring 2010, http://www.ict.org.il/LinkClick.aspx?fileticket=Q-dvDwLODkc%3d&tabid=68.

provide for enhanced communication, and the asymmetries of irregular warfare present the opportunities to capitalize on such strengths. As a result, understanding how networks fight is crucial to determining how to fight them.

B. OVERVIEW

The application of the network concept to the realm of illegal activity and conflict generates such descriptions as terrorist and guerrilla networks, trans-national criminal networks, and even such generally descriptive terms as dark networks and violent networks. Security studies increasingly reference networks to not only describe aspects of insurgency, terrorism, and crime, but also to provide a vehicle for analysis and facilitation of measures of effectiveness. This study proposes and uses the term "fighting network" to describe these illegal, violent networks more accurately and fully that in many ways blur traditional distinctions of illicit activity. Within the study of international relations, these fighting networks are classified as non-state actors, and are usually separated from peaceful non-governmental organizations by the description of violent non-state actors (VNSAs).[2] Notably, recent confrontations with networked opponents have strained the U.S. military, and produced time-intensive, brutally complex, and costly irregular wars in Iraq and Afghanistan. These opponents are the greatest challenge professional militaries face today, and fighting networks are explicitly identified in the most recent U.S. national military strategy, with countering violent extremism listed as the primary national military objective.[3] The challenges that these networked opponents present require a close examination of how they fight, and most importantly, should lead to an understanding of how to counter the threat they pose.

A network is an organizational concept that provides meaning to process and interaction, and is often used to describe a system of linked computer technology. However, the network perspective is much broader than this application. It is a way of

[2] Neal A. Pollard, "Globalization's Bastards: Illegitimate Non-State Actors in International Law," *Law Intensity Conflict & Law Enforcement* 12, no. 3 (2004): 211, http://dx.doi.org/10.1080/0966284042000279009.

[3] U.S. Department of Defense, Joint Chiefs of Staff, *The National Military Strategy of the United States*, February 8, 2011, 4–6.

defining much of how the world works today. In this larger sense, networks, empowered by information technology, powerfully describe many different aspects of social and organizational interaction. The network perspective is one of the defining aspects of modern inquiry in numerous fields and the term "network" is common in everyday usage. According to Jorge Raab and H. Brinton Milward, "the term network has been one of the most widely used notions in the social sciences for the last two decades…," and it can be understood as a description of structure, a label, and as a concept for understanding social activity.[4] In this thesis, the term network will be used broadly to describe organizations defined by certain organizational characteristics, doctrine, operational methods, and information strategy.

Networks are composed of two primary elements, nodes, and the linkages that connect these nodes. The nodes and their connections can be nearly anything, such as people and friendships, computers and communication lines, cities and highways, providing a breadth of application and analysis.[5] This study focuses on social networks composed of individuals, and groups, as nodes and their relationships, which is a critical distinction. While the physical science aspects of network study provide empirical data, leading to more quantitative analysis, the human nature of social networks makes such rigorous conclusions difficult.[6] Moreover, human networks are constantly changing and display fluid behavior influenced by psychological and cultural aspects, which are far less tangible notions than physical structure. Incorporating these distinctions into an idea of networks provides a broad range of typologies united under a common purpose, but are decentralized, exhibit high degrees of autonomy, dispersed communications flow, and informal authority.

Fighting networks transcend many of the classic distinctions in irregular warfare, and they increasingly define the nature of modern conflict. Irregular warfare, also loosely

---

[4] Jorge Raab and H. Brinton Milward, "Dark Networks as Problems," *Journal of Public Administration Research and Theory*," (October 2003): 417.

[5] Mark Newman, Albert-László Barabási, and Duncan J. Watts, ed., *The Structure and Dynamics of Networks* (Princeton, NJ: Princeton University Press, 2006), 3.

[6] Robert G. Spulak, Jr. and Jessica Glicken Turnley, "Theoretical Perspectives of Terrorist Enemies as Networks," *Joint Special Operations University Report 05-03* (Hurlburt Field, FL: Joint Special Operations University Press, 2005), 10.

referred to as unconventional warfare, partisan war, guerrilla warfare, or characterized by "small wars," is a timeless aspect of human conflict that despite its many variations, has exhibited constant themes.[7] Regardless of its many forms, the most salient characteristic of modern irregular warfare is the networked structure of most opponents. The networked form is uniquely suited to take advantage of the "engines of globalization," which are primarily characterized by modern information technology.[8] While traditional measures reveal an asymmetric disparity between large nation-states and weaker opponents, modern information technology provides capabilities that enhance the ability of the latter despite this difference. The combination of timeless, irregular warfare characteristics and modern technology creates a synergy that produces increasingly dangerous opponents. Countering these irregular opponents requires a detailed understanding of the organization, doctrine, operational methods, and use of information, which both empowers networks and may reveal vulnerabilities.

This research employs a theoretical framework that draws on the rich bodies of knowledge informing network theory, network-based operations, irregular warfare, organizational theory, and information strategy. Initially, examining each of these theoretical areas produces a detailed description of how networks fight. The second part of this analytic framework creates hypotheses focused on how to counter networks. The primary methodology employed in this study is comparative case studies focused on a cluster of networks engaged in irregular warfare. This cluster consists of three cases, each marked by "tough opponents," and network-based organizations operating in the information age: the Chechen separatists, Lebanese Hezbollah, and Al-Qaeda in Iraq. These cases test the hypotheses generated in the second portion to understand better how to confront networks effectively in irregular conflict.

---

[7] Lewis H. Gann, *Guerrillas in History* (Stanford, CA: Hoover Institution Press, 1971), 1. Gann's work provides a concise, yet heuristic, view of the timeless qualities of guerrilla warfare. Other notable surveys include Walter Laqueur, *The Guerrilla Reader* (New York, 1977); John Ellis, *A Short History of Guerrilla Warfare* (London, 1975); Robert B. Asprey, *War in the Shadows: The Guerrilla in History* (New York, Doubleday & Company, Inc., 1975); Gerard Chaliand, ed. *Guerrilla Strategies: An Historical Anthology from the Long March to Afghanistan* (Berkley: University of California Press, 1982).

[8] Pollard, "Globalization's Bastards," 215.

C. PURPOSE AND SCOPE

The purpose of this thesis is to understand how networks fight, and how to counter networks that engage in irregular warfare. Overall, this thesis seeks to provide a deeper understanding of irregular warfare, viewed through the network perspective, and to advance theory in a way that generates a better understanding of how to counter networked opponents. As the information age unfolds, nation-states are increasingly challenged by violent, non-state actors, most of which organize, operate, and fight in non-conventional ways. It is these attributes that challenge formal militaries and that provide networked opponents their ability to pose such great risks to security and stability. While this basic challenge is readily recognized, a lack of overall awareness and understanding exists about how best to counter these fighting networks. In addition, traditional characterizations of these threats as guerrillas, or in terms of insurgent goals and strategies, provide only a limited perspective of the overall threat. By focusing on fighting networks, this thesis illustrates the importance and transformative nature of network-style warfare, and addresses ways to counter these networks.

While the network perspective is expansive, this thesis focuses on fighting networks in irregular warfare, and the scope of the study is designed to provide insights into this arena of conflict. To describe and analyze networks, the integration of multiple methods and approaches is necessary. In addition, it must be emphasized that many tools exist that must be employed against the complex problem sets of irregular warfare. A focus on countering networked opponents is but one aspect of a comprehensive effort to ensure security and stability. In this regard, this study focuses on addressing the immediate threats that networked opponents pose, and gives secondary emphasis to the deeper roots of conflict, such as ideological differences, cultural clashes, and popular grievances. Still, efforts to understand the broader aspects of social networks and their cultural environment provide vital support. Moreover, a clear recognition exists that the focus on countering fighting networks must be synchronized and integrated with efforts that seek to correct the fundamental origins of conflict.

D. RESEARCH QUESTION

- How do networks fight, and how do we fight the networks that increasingly define irregular warfare?

The preliminary question that must be addressed is what is a network? Also, what characteristics make it possible to describe certain organizational attributes as network-based? An understanding of the network perspective is required to know what constitutes a network. From this point, the study of network capabilities provides a means to address how fighting networks might use conflict to achieve their aims. In essence, the first part of the research question seeks to understand the organizational characteristics, doctrine, operational methods, and information strategy that these opponents employ to fight. The second part of the question is contingent on an understanding of how networked opponents fight. This understanding provides the basis for proposing organizational attributes, doctrine, and operational methods that exploit vulnerabilities and provide effective ways to counter fighting networks.

E. THEORETICAL FRAMEWORK

This thesis design draws on multiple bodies of knowledge to provide a theoretical framework for generating hypotheses. This framework employs the network perspective in conjunction with an understanding of irregular warfare to generate a combined concept that answers the research question. The theoretical framework that informs this research consists of the following areas of knowledge: network theory, network-based operations, irregular warfare, organizational theory, and information strategy. Each of these bodies of knowledge provides insight into fighting networks and their interaction in the realm of current warfare, and a closer examination generates testable hypotheses.

Network theory provides the starting point for theoretical research. This rapidly expanding field answers the question of what constitutes networks, and provides descriptions for further analysis. A combination of mathematic and scientific discoveries over the last 50 years provides the basis for network theory, which seeks to provide

"…insights into the structure and workings of complicated networks."[9] These discoveries form an exciting and novel perspective about numerous interactions, both social and physical, in today's world. The noted physicist Albert-László Barabási describes network theory as "the next scientific revolution."[10] In addition to the scientific breakthroughs, network theory is providing impetus to various aspects of social science, including social network theory and actor-network theory. An understanding of network principles provides a foundation for examining how networks fight, and is critical to formulating ways to counter them. This focus on network theory seeks to define key principles governing networks and establish their essential attributes. One of the unique aspects of network theory is the universality of key characteristics, such as connectivity, centrality, order, and growth. The fact that biological, computer science, and social networks all share fundamental principles suggests common attributes governing networks, and contributing to their effectiveness.

Network research in the last several decades reveals that, despite differences in substance and form, network architecture possesses fundamental characteristics.[11] These characteristics form the following milestones in the development of network theory. While the numerous discoveries by a network of scientists are too many to list, the basic milestones are: the degree of separation experiments (Stanley Milgram, 1967), the importance of clustering and weak links (Mark Granovetter, 1973), the small-world model (Duncan Watts and Steve Strogatz, 1998), the role of hubs and free-scale networks (Albert-László Barabási and Rika Albert, 1999), and the ideas of competition and growth in networks (Ginestra Bianconi and Albert- László Barabási, 2001).[12] In the social

---

[9] Mark Buchanan, *Nexus: Small Worlds and the Groundbreaking Theory of Networks* (New York: W.W. Norton & Company, Inc., 2003), 18.

[10] Albert-László Barabási, *Linked: The New Science of Networks* (Cambridge, MA: Perseus Books, 2002), 8.

[11] Buchanan, *Nexus*, 15.

[12] Stanley Milgram, "The Small World Problem," *Psychology Today* (1967): 60–67; Mark Granovetter, "The Strength of Weak Ties," *American Journal of Sociology* (1973): 1360–1380; Duncan Watts and Steve Strogatz, "Collective Dynamics of 'Small-World' Networks," *Nature* (1998): 440–442; Albert-László Barabási and Rika Albert, "Emergence of Scaling in Random Networks," *Science* (1999): 509–512; Ginestra Bianconi and Albert-László Barabási, "Competition and Multi-scaling in Evolving Networks, "*Europhysics Letters (EPL)* (2001): 436–442.

sciences, social network analysis utilizes network theory discoveries, and forms the basis for much of the research on networks. Social network analysis is "a mathematical method for 'connecting the dots'…[that] allows us to map and measure complex, sometimes covert, human groups and organizations."[13] Yet, rather than focus exclusively on the inner-workings of networks, this study incorporates a broader understanding of network theory to refine and advanced principles of networks in conflict.

The second base of theoretical knowledge that informs this research is network-based operations. The study of network-based operations seeks to clarify how networks operate, and clearly distinguishes between different uses of the network perspective. This theoretical concept provides structure and meaning for network-based conflict, and adds an operational dimension to the idea and concept of networks in conflict. The idea of network-based operations stems from the concept of network-style warfare, or "netwar," first proposed by John Arquilla and David Ronfeldt. This study develops this idea beyond the concept level, providing operational insights focused on fighting networks in irregular warfare.[14] It is important to distinguish that this conceptual framework is different from the United States (U.S.) Department of Defense's Network-Centric Warfare (NCW) concept, which seeks increasing awareness and control in a system that links decision makers with sensors and shooters.[15] NCW focuses on technological connections, which provide situational awareness for a shared network of war-fighting systems. Instead, network-based operations go beyond the physical architecture designed to achieve control, and recognizes that networks operate in ways that are often random, decentralized, and self-empowered. Further, network-based operations are increasingly recognized as the most suitable concept for achieving sustainable partnership networks

[13] Valdis Krebs, "Mapping Networks of Terrorist Cells," *Connections* 24, no. 3, 45, http://www.sfu.ca/~insna/Connections-Web/Volume24-3/Valdis.Krebs.web.pdf.

[14] John Arquilla and David F. Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: RAND, 1996). Also see John Arquilla and David Ronfeldt, ed., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, 1997); John Arquilla and David Ronfeldt, ed., *Network and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001).

[15] Vice Admiral Arthur Cebrowski and John Garstka, "Network-Centric Warfare," *Proceedings* 24, no. 1, (United States Naval Institute Press, 1998), 28–35.

that unite numerous actors against complex problems.[16] Ironically, these two very different concepts are often conflated, but their most distinguishing characteristic is that while NCW seeks to eliminate the "fog of war," through superior technology and information dominance; network-based operations are characterized by fluidity and recognize that fog and friction are fundamental conditions of war.[17] In addition, while network-based operations recognize the empowerment of modern information technology, they are characterized by a holistic approach that incorporates multiple aspects, such as organization, leadership, doctrine, information strategy, and social factors. Network-based operations both inform and are robustly developed throughout the course of this study.

The information revolution has provided tremendous strength to networked forms of organization.[18] "Like the large numbers of private corporations that have embraced IT [information technology] to operate more efficiently and with greater flexibility, terrorists are harnessing the power of IT to enable new operational doctrines and forms of organization." [19] The proliferation of computer and cellular communications technology provides decentralized, informal organizations the means to achieve greater impact on the battlefield. Most terrorist and insurgent organizations are characterized by network-based organization and doctrine, and the netwar concept proposes, "it takes networks to fight networks."[20] If this is the case, those seeking to counter networks should, it seems logical, employ network-based operational principles. The degree to which this is true may correlate with operations that successfully degrade enemy networks, and conversely,

---

[16] David T. Johnson, Assistant Secretary, U.S. State Department, "Fighting Networks with Networks: Partnership and Shared Responsibility on Combating Transnational Crime," Keynote Speech, Trans-Pacific Symposium on Dismantling Illicit Networks, Honolulu, Hawaii, November 10, 2009, http://www.state.gov/p/inl/rls/rm/131805.htm.

[17] An example of this mixing of concepts is the Joint Special Operations University Report, "Implications for Network-Centric Warfare," which provides an excellent examination of network-based operations, but under the NCW moniker. Jessica Glicken Turnley, "Implications for Network-Centric Warfare," *Joint Special Operations University Report 06-3* (Hurlburt Field, FL: Joint Special Operations University Press, 2006).

[18] Arquilla and Ronfeldt, *Networks and Netwars*, 1.

[19] Michele Zanini and Sean Edwards, "The Networking of Terrorism in the Information Age," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND Corporation, 2001), 30.

[20] Arquilla and Ronfeldt, *Networks and Netwars*, 15.

a lack of network-based operations may prevent the degradation of an adversary network. Yet, this hypothesis may not be sufficient and other aspects of both organizational theory, such as hierarchical forms, and doctrine, may be able to counter networks.[21] The focus on network-based operational theory provides a framework to establish critical vulnerabilities of network-based organizations, and assists in defining those key tasks essential to attacking those vulnerabilities. Despite a growing understanding of networks, little discussion occurs of how networks actually engage in conflict, or descriptions of their doctrinal methods at the operational level, which is not a new phenomenon in war, as doctrine generally lags behind the development of new technologies and concepts.

The study of irregular warfare forms the third theoretical basis for an examination of the research question. Networks are prevalent in the irregular warfare environment, and a study of its dynamics seeks to understand why this is the case. Irregular warfare is doctrinally defined as "a violent struggle against state and non-state actors for legitimacy and influence over the relevant population(s). Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, in order to erode an adversary's power, influence, and will."[22] According to U.S. military joint doctrine, irregular warfare consists of five core activities: counter-terrorism, unconventional warfare, foreign internal defense, counter-insurgency, stability operations, and numerous related activities.[23] The Department of Defense definition of unconventional warfare (UW) provides a primary source for formal doctrine describing the antagonist's perspective in much of irregular warfare, which is fundamentally unconventional to the point that the two terms are used interchangeably outside of formal

---

[21] David Tucker, "Terrorism, Networks, and Strategy: Why the Conventional Wisdom is Wrong," in *Homeland Security Affairs* 4, no. 2 (June 2008): 2, http://www.hsaj.org/?article=4.2.5.

[22] U.S. Department of Defense, *Irregular Warfare: Countering Irregular Threats Joint Operational Concept v.2.0* (Washington, DC: U.S. Government Printing Office, 2010), B–2; U.S. Department of Defense, Department of Defense Directive 3000.7; *Irregular Warfare*, (Washington, DC: U.S. Government Printing Office, 2008), 11; U.S. Department of Defense, Joint Publication 1-02, *Dictionary of Military and Associated Terms* (JP 1-02), (U.S. Government Printing Office, 2009), 280.

[23] Each of these terms has specific doctrinal definitions based on the application of U.S. military force. For instance, guerrilla warfare, which is the most frequently used term to describe irregular warfare activity, is not included because unconventional warfare (UW) defines an advisory effort in support of guerrilla activity, not unilateral guerrilla action. Written to support a larger traditional warfare framework, these tightly defined doctrinal definitions leave out a large range of special operations and paramilitary activity. "*Irregular Warfare: Countering Irregular Threats," Joint Operational Concept v. 2.0,* 5.

military doctrine. While a great degree of attention is given to irregular warfare, its current focus only defines the nature of operations, and uses terms, such as asymmetric threats, non-linear conflict, or doctrinal categories, such as counter-terrorism (CT) or counter-insurgency (COIN). The purpose of focusing on irregular warfare is to understand how networked opponents fight. The initial portion of this study on networks in irregular warfare is informed by aspects of guerrilla warfare and UW, and the second portion examines CT and COIN.

Irregular Warfare Doctrinal Terminology	
Irregular Warfare (IW)	A violent struggle among state and non-state actors for legitimacy and influence over the relevant populations. Irregular warfare favors indirect and asymmetric approaches, although it may employ the full range of military and other capabilities to erode an adversary's power, influence, and will. (Joint Publication 1, MAR 09).
Unconventional Warfare (UW)	Activities conducted to enable a resistance movement or insurgency to coerce, disrupt or overthrow a government or occupying power by operating through or with an underground, auxiliary, or guerrilla force in a denied area. (Training Circular 18-01, DEC 10).
Counter-Insurgency (COIN)	Comprehensive civilian and military efforts taken to defeat an insurgency and to address any core grievances. (Joint Publication 3-24, OCT 09)
Counter-Terrorism (CT)	Actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks. (Joint Publication 3-26, NOV 09).
Guerrilla Warfare	Military and paramilitary operations conducted in enemy-held or hostile territory by irregular, predominantly indigenous forces. (Joint Publication 3-05.1, APR 07).
Insurgency	The organized use of subversion and violence by a group or movement that seeks to overthrow or force change of a governing authority. (Joint Publication 3-24, OCT 09).
Terrorism	The calculated use of unlawful violence or the threat of unlawful violence to inculcate fear; intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political religious, or ideological (Joint Publication 3-07.2, APR 06).

Table 1. Current Irregular Warfare Terminology According to U.S. Military Doctrine

UW is a formal doctrinal term that expresses an advisory relationship in what has traditionally been the defining characteristic of irregular warfare—guerrilla warfare. Guerrilla warfare is a set of tactics and techniques that have consistently been the choice of weaker opponents who seek to oppose the strong (usually formal governments), and seeks to avoid direct confrontation by relying on speed and surprise in attacks. For most of history, guerrilla warfare was seen as a minor aspect of war, and not one that could be used against a regular military. Despite its use as a reaction against European colonial expansion, it remained a largely secondary means of conflict until after World War II, when it was paired with anti-colonial liberation, and used by theorists, such as Mao Tse-Tung in a revolutionary manner.[24] In addition, terrorism is also employed as a tactic, often in conjunction with guerrilla warfare, but also as a single means of political violence.[25]

Fighting networks, including terrorist, insurgent, and even foreign-state-sponsored networks seek to defeat their opponents using terrorism and other asymmetric tactics. Counter-terrorism is one of the current leading aspects of irregular warfare, and it seeks to defeat terrorist-based threats. An examination of CT literature shows that a void exists in how to defeat terrorist networks systematically, with discussions focused on leadership targeting, reconciliation, repression, and even how fighting networks sometimes defeat themselves.[26] Recently, the term CT has been taken to mean an exclusive focus on countering an enemy threat directly, using primarily kinetic means. This focus usually takes the form of direct leadership targeting, or an emphasis on killing or capturing high-value targets (HVTs). However, very little discussion of the operational approaches required to disrupt, and perhaps defeat, an entire networked organization occurs.

COIN is the most examined aspect of irregular warfare, and most COIN studies emphasize an indirect approach that places the population's loyalty as an essential condition to success. Classic scholars of counter-insurgency, such as David Galula, Julian Paret, and Roger Trinquier, all argue that the population's support is essential to ensuring

---

[24] Chaliand, ed. *Guerrilla Strategies,* 7.

[25] Ibid., 30.

[26] Martha Crenshaw, "How Terrorism Declines," *Terrorism and Political Violence* 3, no. 1 (1991): 47.

control in counter-insurgency.[27] More recent authors, such as John Nagl and David Kilcullen, agree, and stress the importance of providing security for the population, as a part of a comprehensive framework.[28] However, a focus on "nation-building" has tended to produce an overemphasis on a "hearts and minds" campaign in COIN, resulting in failures to address networked insurgent forces fully.[29] Most classical counter-insurgency strategy promotes a comprehensive approach that seeks to both secure the local population and defeat their networked opponent. In this regard, while CT and COIN may serve as useful distinctions, their primary activities are both essential aspects within a larger struggle for control in an irregular warfare environment. This struggle for control, and its direct relationship with legitimacy, is succinctly described in Gordon McCormick's "Diamond" COIN model, which describes the application of both indirect and direct means to counter-insurgent organizations.[30] This model provides the clearest depiction of the fact that modern distinctions of COIN and CT separate what are really two key aspects of counter-insurgency; elements that must be synchronized for effective counter-insurgency.

The common end-state of irregular warfare is the defeat of a network-based enemy organization, marked by their loss of control over the population. While historical examples may lack certain characteristics of modern-day networks, the doctrinal principles remain the same. A focus on irregular warfare provides numerous aspects of CT and COIN from which to analyze examples of counter-network operations. The irregular warfare lens informs this study by providing insight into optimal methods for conducting counter-network activities in an irregular warfare environment.

---

[27] David Galula, *Counterinsurgency Warfare Theory and Practice* (New York: Praeger Publishers, 1968); Julian Paret, *Counter-Insurgency Operations: Techniques of Guerrilla Warfare* (New York: Walker and Company, 1967), 176; Roger Trinquier, *Modern Warfare: A French View of Counterinsurgency*, PSI Classics of the Counterinsurgency Era (Westport, CN: Praeger Security International, 2006).

[28] David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (New York: Oxford University Press, 2009), 266; John Nagl, *Learning to Eat Soup With a Knife: Counterinsurgency Lessons from Malaya and Vietnam* (Westport, CT: Praeger Publishers, 2002), 83.

[29] John P. Sullivan and Adam Elkus, "Strategy and Insurgency: An Evolution in Thinking?" http://www.opendemocracy.net/.

[30] Gordon McCormick, "Diamond Insurgent/COIN Model," depicted in Eric P. Wendt, "Strategic Counterinsurgency Modeling," *Special Warfare* 18, no. 2 (September 2005): 5–6.

Aspects of organizational theory form another theoretical perspective, and provide insight into what empowers network-based operations. The use of network-based organizational structure is one of the defining characteristics of the primary threats in irregular warfare. As Sean Edwards and Michele Zanini note, "just as companies in the private sector are forming alliance networks to provide complex services to customers, so too are terror groups 'disaggregating' from hierarchical bureaucracies and moving to flatter, more decentralized, and often changing webs of groups united by a common goal."[31] Organizational theory provides insight into aspects of organizational structure, environmental interaction, and important human resource dynamics, such as leadership. Furthermore, organizational theory provides a well-developed conceptual basis to understand the interaction of aspects of size, decentralization vs. centralization, and span of control.[32] The primary aspect of organizational theory that examines the shaping of organizations is contingency theory, and it seeks to "predict the performance or effectiveness of an organization based on the extent to which the organization's structure matches contextual contingencies such as organizational size, technology, and the environment."[33] Each of these contingencies presents characteristics within organizations and provides insight into network-based organizations.

The study of information strategy provides additional theoretical knowledge, and it shapes both the conduct of information operations, including the use of intelligence, and the employment of information technology. The rise of information technology empowers both operational action within irregular strategy and expands the network-based opponent's capacity to conduct information warfare. Information warfare consists of seven forms: Command-and-Control Warfare (C2W), Intelligence-based Warfare (IBW), Electronic Warfare (EW), Psychological Warfare, "Hacker" Warfare, Economic Information Warfare (EIW), and Cyberwarfare.[34] A conventional military's strengths in

---

[31] Zanini and Edwards, "The Networking of Terrorism in the Information Age," 30.

[32] Steven L. McShane and Mary Ann Von Glinow, *Organizational Behavior* (Boston: McGraw-Hill Irwin, 2007), 22.

[33] Abdulkader H. Sinno, *Organizations at War in Afghanistan and Beyond* (Ithaca, NY: Cornell University Press, 2008), 9.

[34] Martin Libicki, *What is Information Warfare?* (Washington, DC: National Defense University, U.S. Government Printing Office, 1995), Preface.

C2W, IBW, and EW are based primarily on conflicts involving traditional doctrine and strategies that emphasize technological advantages in Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), as well as a corresponding degree of precise and overwhelming firepower. In keeping with the asymmetric nature of irregular warfare, these strengths provide mixed relative advantages against a dispersed, networked organization. Network-based organizations use different methods within these forms to gain advantages in the asymmetric nature of irregular warfare. In addition to providing a framework for the information dimension of conflict, information strategy is essential in understanding the strengths and weaknesses that the proliferation of information technology presents for network forms. Examining the information strategy of network-based organizations provides further insights into the important nature of information in how networks fight.

F. METHODS

The primary method employed for this research is comparative case studies that focus on networks in irregular warfare contexts. These case studies are employed as a part of a congruence process, where the theory derived from directly examining the research question in the initial chapters is evaluated based on its ability to explain outcomes in each case.[35] A cluster of cases was chosen for this study for the following reasons: they are examples of irregular warfare, they display the capabilities of the networked opponent, and they are empowered by information technology. Another consideration common to each of the cases is that they provide examples of "robust" opponents, and therefore, serve as tough tests of attempts to counter networks. There are other examples of networked threats, and certainly numerous insurgent and terrorist examples throughout history. However, a unique aspect of the fighting organizations in these cases is their ability to use information technology in ways that dramatically empower their networked aspects.

[35] Alexander L. George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences* (Cambridge, MA: MIT Press, 2005), 181.

The first case study focuses on the Russian conflict with Chechen opponents in both the 1st Russo-Chechen War (1994–1996) and the 2nd Russo-Chechen War (1999–present). The 1st Russo-Chechen War had its origins in the Chechen declaration of independence in the wake of the 1991 Boris Yeltsin-inspired autonomy movement.[36] After the brutal 1st conflict, and following an uneasy period of relative quiet, the 2nd Russo-Chechen War began with an Islamic-extremist-led offensive movement into neighboring Dagestan.[37] While the Russian government states that the war ended in 2009, most observers believe that it has simply entered a new phase, marked by dispersed and lethal terrorist attacks in the Russian heartland and a spread into neighboring provinces.[38] This case is noteworthy for the ability to contrast Russian and Chechen efforts in two separate episodes of this conflict, and to study the evolving nature of the networked challenge.

The second case study focuses on the Israeli conflict with Lebanese Hezbollah, and in particular, analyzes the results of the 2006 Israeli-Hezbollah clash in Lebanon. From its inception in the early 1980s, Hezbollah has been a non-state actor, acting with support from various sources, but always characterized by a popular socially based militant movement focused on resisting the actions of Israel and its supporters.[39] In this sense, it is an instructive case, because it highlights the character of irregular warfare, and a non-state actor challenging national powers by directly confronting their military forces. Israel invaded southern Lebanon in 1978 and in 1982 to deny the area to the Palestinian Liberation Organization. The start of a withdrawal from southern Lebanon in 1985 coincided with the formation of, and direct challenges from, an increasingly aggressive Hezbollah network, and by 2000, Israel had withdraw its forces back to its formally recognized border. The 2006 conflict marked the start of a second overt clash, and began with Hezbollah's daring raid into Israel to ambush an Israeli motorized patrol,

[36] MAJ Raymond C. Finch, "Why the Russian Military Failed in Chechnya," *Foreign Military Studies Office Special Study 98–16* (Fort Leavenworth, KS: Center For Army Lessons Learned, 1998), 1.

[37] Paul Murphy, *The Wolves of Islam* (Washington, DC: Brassey's Inc., 2004), 2.

[38] Brendan Fogarty, "Chechnya Redux? Violent Conflict in Ingushetia." *Harvard International Review* 31, no. 4 (January 1, 2010): 8, http://www.proquest.com.libproxy.nps.edu/.

[39] Augustus Richard Norton, *Hezbollah* (Princeton, NJ: Princeton University Press, 2007), 38.

resulting in the capture of two soldiers and the killing of three others. The conflict that followed highlights a further evolution in methods and aspects of irregular warfare, to the extent that some observers have called it a classic example of a "hybrid-war."[40] One of the commonly referenced aspects of hybrid warfare is the super-empowered network characteristics of its opponents, and this case study is expected to provide unique insights into the nature of these conflicts.

The third case study focuses on the United States and Iraqi struggle against Al-Qaeda in Iraq from 2004–present. The U.S. invasion of Iraq in 2003 prompted an Iraqi-led popular insurgency, which grew in scope and diversity to include numerous insurgent groups. One of the catalytic groups, and perhaps most powerful, was Al-Qaeda in Iraq, which was recognized as a part of the Al-Qaeda network by Osama bin Laden in December 2004.[41] Al-Qaeda in Iraq sought increasing control and organizational supremacy over the insurgency in Iraq, as seen in violent clashes with other insurgent groups and the formation of its umbrella organizations, the Mujahedin Shura Council (MSC) and the Islamic State of Iraq (ISI).[42] By examining the conflict with al-Qaeda in Iraq in two phases, from 2004–mid 2006, and from 2006 until the present, unique aspects of the conflict present themselves, including the role of the Sunni tribal awakening, and the U.S. surge in forces. Al-Qaeda in Iraq's violent tactics, use of information operations, and quest for organizational control combine to make it a unique network opponent. The study of this organization and the efforts to counter it provide a clear example of a conflict with a network-based opponent, and its current nature provides for a depth and richness of study.

An examination of these conflicts highlights the organizational characteristics, doctrine, operational methods, and information strategies that characterize each of these network-based opponents. These examples generate insights to compare against and test

---

[40] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), 35.

[41] Ahmed S. Hashim, *Insurgency & Counter-insurgency in Iraq* (Ithaca, NY: Cornell University Press, 2006), 143.

[42] Evan F. Kohlman, "State of the Sunni Insurgency in Iraq," http://www.nefafoundation.org/index.cfm?pageID=24.

hypotheses. Within each of these case studies, a process tracing method reveals the presence of a causal chain between various hypotheses-derived independent variables, and the dependent variable of effectively countering networks. Process tracing seeks to "identify a causal path that depicts how the independent variable leads to the outcome of the dependent variable."[43] Overall, this occurs in a four-stage process, with the first stage focused on how networks fight, and the second stage using that analysis to identify variables leading to a counter-network framework. These causal relationships are tested in the third stage with an examination of each case study. Finally, a comparative analysis of the case studies is used to modify previous results and produce counter-network theory and recommendations.

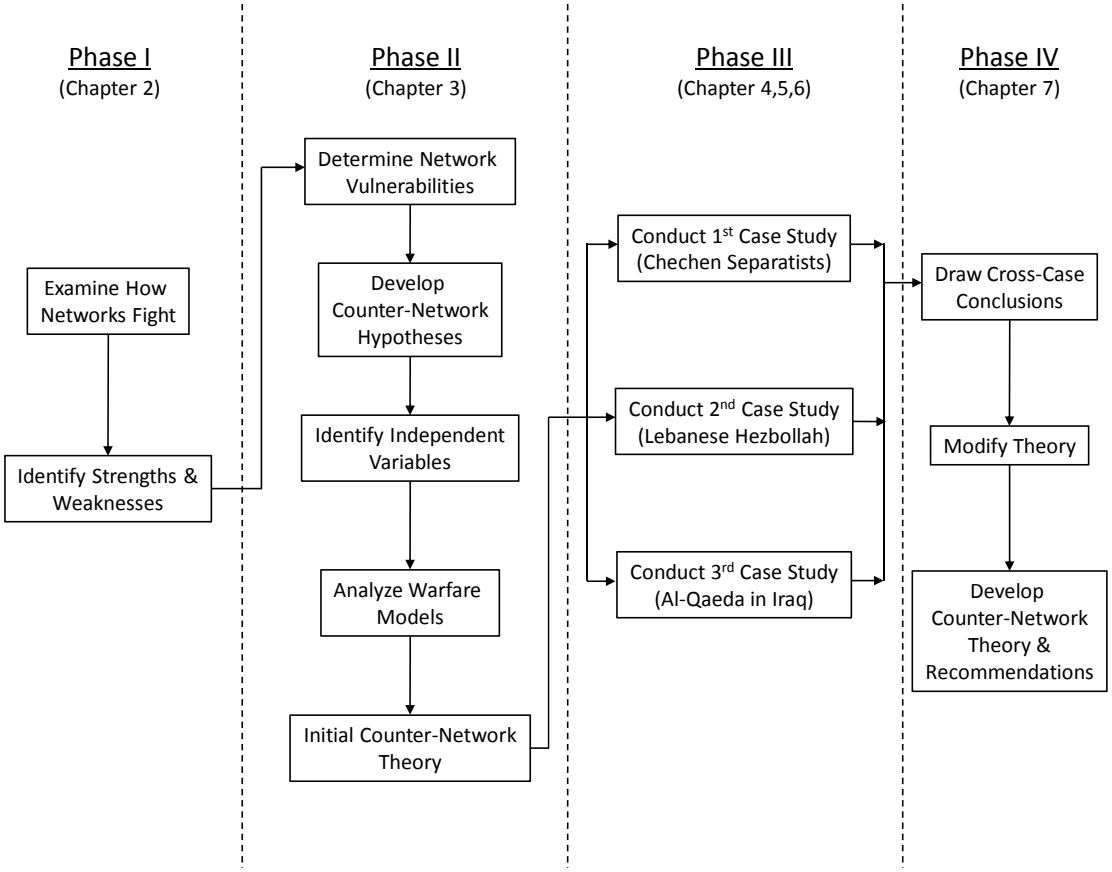

Figure 1. Thesis Methodology Flowchart

[43] George and Bennett, *Case Studies and Theory Development in the Social Sciences*, 183.

II. HOW NETWORKS FIGHT

> What is of supreme importance in war is to attack the enemy's strategy. Therefore, I say: know your enemy and know yourself and in a hundred battles you will never be in peril.[44]
>
> - Sun Tzu

A. THE RISE OF NETWORKS IN IRREGULAR WARFARE

The modern age is witnessing a revolution in irregular warfare, with dispersed non-state actors wielding more power and confronting modern professional militaries in new and innovative ways. "Without a shadow of a doubt, the terrorist attacks of 9/11 encapsulate a new form of waging war in a manner that circumvents traditional defence postures—ones geared toward protecting the nation from the armed forces of another state, not cosmopolitan and sophisticated terrorists."[45] The networks that violently confront nation-states pose the defining challenge of modern irregular warfare.[46] These fighting networks utilize network-style warfare to confront superior opponents, are capable of dramatic change, and adaptable enough to incorporate multiple forms of strategy and tactics. John Robb calls these modern networks "global guerrillas," because "this new method of warfare offers clear improvements (for our enemies) over traditional terrorism and military insurgency."[47] Another attempt to characterize this challenge

---

[44] Sun Tzu, *The Art of War*, trans. and ed. Samuel B. Griffith (London: Oxford University Press, 1971), 77, 84.

[45] Alastair Finlan, *Special Forces, Strategy and the War on Terror: Warfare by Other Means* (New York: Routledge, 2007), 112.

[46] For more on the clashes between nation-states and these networked opponents see, Manuel Castells, *The Rise of the Network Society* (Cambridge, MA: Blackwell, 1996); Mark Duffield, "War As a Network Enterprise: The New Security Terrain and Its Implications," *Cultural Values* 6, no. 1, (2002): 153–165, http://www.idrc.ca/uploads/user-S/10588048681Duffield_netwar2.pdf, 161; Arquilla and Ronfeldt, *Network and Netwars: The Future of Terror, Crime, and Militancy*; Michael Kenney, *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation* (University Park, PA: Pennsylvania State University Press, 2007); Audrey Kurth Cronin, "Behind the Curve: Globalization and International Terrorism," *International Security* 27, no. 3 (Winter 2002/2003): 30–58; Marc Sageman, *Understanding Terror Networks* (Philadelphia, PA: University of Pennsylvania Press, 2004); Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 2006), 229–295.

[47] John Robb, *Brave New War* (Hoboken, NJ: John Wiley & Sons, 2007), 14–15.

describes these opponents as "techno-guerrillas."[48] In fact, fighting networks may utilize some guerrilla warfare techniques, but they are not constrained by many of the traditional limitations of irregular warfare. Insurgent goals, terrorist tactics, or a blend of forms may characterize these networks, but they fight in an unconventional manner, a manner best described by the netwar concept.[49] The netwar concept emphasizes the irregular nature of networks in conflict, featuring "small, dispersed units that can deploy nimbly," with the ability to "penetrate and disrupt, as well as elude and evade."[50]

In addition to their organizational features, the ability of irregular opponents to achieve adaptable power is based primarily on their utilization of modern information technology in a synchronized method of fighting that is a product of the modern information age. Information technology provides tremendous empowerment by allowing further connections and communication, while at the same time, increasing a network's ability to remain de-centralized. Rapid innovation in modern information technology is changing multiple aspects of warfare, making politically motivated violence more potent and increasing the spectrum of capabilities available to all combatants. However, the dramatic rate of technological changes favor networks more than their opposition, because they create new asymmetries beyond just force considerations.[51] Moreover, it is not just that modern technologies super empower networks; these networks use the latest technologies themselves as weapons, with aircraft turned into guided missiles, cellular technology used to detonate improvised explosive weapons, and computers facilitating cyber attacks against a spectrum of targets.[52] These networked opponents use information technology as a tool, but it is essential to recognize that every aspect of their fighting is synchronized and "attuned to the information age."[53]

---

[48] Clyde Roston, "Terrorist to Techno-Guerrilla: The Changing Face of Asymmetric Warfare," *Joint Center for Operational Analysis Journal* 10, no. 1 (United States Joint Forces Command, December 2007), 45.

[49] Arquilla and Ronfeldt, *The Advent of Netwar*.

[50] Arquilla and Ronfeldt, *Networks and Netwars*, v.

[51] Thomas Rid and Marc Hecker, *War 2.0: Irregular Warfare in the Information Age* (Westport, CT: Praeger Security International, 2009), 126–128.

[52] Robb, *Brave New War*, 11.

[53] Arquilla and Ronfeldt, *Networks and Netwars*, 7.

Fighting networks display timeless characteristics of irregular opponents, such as terrorists, guerrillas, and insurgents, but are best defined by their synthesis of tactics and use of modern information technology in ways that provide unique advantages. These networks represent the violent, lawless side of network forms, which also includes social networks that organize and operate under many of the same principles. Like other social networks, the decentralized nature of networks in irregular warfare is possible, and enhanced by combinations of social linkages, more than formal, hierarchical structures. Bruce Hoffman describes the modern terrorist threat as being, "…a new breed of terrorist entity to which traditional organizational constructs and definitions do not neatly apply."[54] Arquilla and Ronfeldt's initial description of the netwar concept highlights the characteristics that define networks in irregular warfare:

> an emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrine, strategies, and technologies attuned to the information age. These protagonists are likely to consist of dispersed organizations, small groups, and individuals who communicate, coordinate and conduct their campaigns in an internetted manner, often without precise central command.[55]

While the unprecedented scale of the 9/11 al-Qaeda attacks galvanized public attention, the terror networks of the 1970s and 1980s provided an initial indicator of the potential power of these loosely coupled organizational forms. In 1981, Claire Sterling described "…an international terrorist circuit, or network, or fraternity," that was not necessarily welded in a formal structure, but whose elements were "linked.""[56] More recently, some theorists have even gone so far as to propose networked opponents as a significant element in a new generation of warfare, most notably William Lind, in his description of 4th Generation Warfare (4GW).[57] However, much of what characterizes

---

[54] Hoffman, *Inside Terrorism*, 38.

[55] Arquilla and Ronfeldt, *Networks and Netwars*, 6.

[56] Claire Sterling, *The Terror Network: The Secret War of International Terrorism* (New York: Holt, Rinehart, and Winston, 1981), 10.

[57] William S. Lind, "Understanding Fourth Generation Warfare, *Military Review* 84, no. 5 (2004): 12–16; Colonel Thomas X. Hammes, *The Sling and the Stone: On War in the 21st Century* (St. Paul, MN: Zenith Press, 2004).

these networks is not a generational leap in warfare, but a distinctly different form of irregular warfare with unique characteristics derived from innovations in organization, doctrine, and modern technology. Network-style warfare is truly a "paradigm shift," much like the scientific breakthroughs in network theory, and is an excellent example of this phrase, first proposed by Thomas Kuhn in *The Structure of Scientific Revolutions* to describe such breakthroughs.[58] Fighting networks meld the timeless elements of unconventional warfare with modern information technology to produce a blend of organization, doctrine, operations, and strategy that are challengingly sophisticated. Yet, unlike traditional unconventional threats, these fighting networks achieve success with organizational and doctrinal features synchronized and in-stride with the rapid changes of the information age.

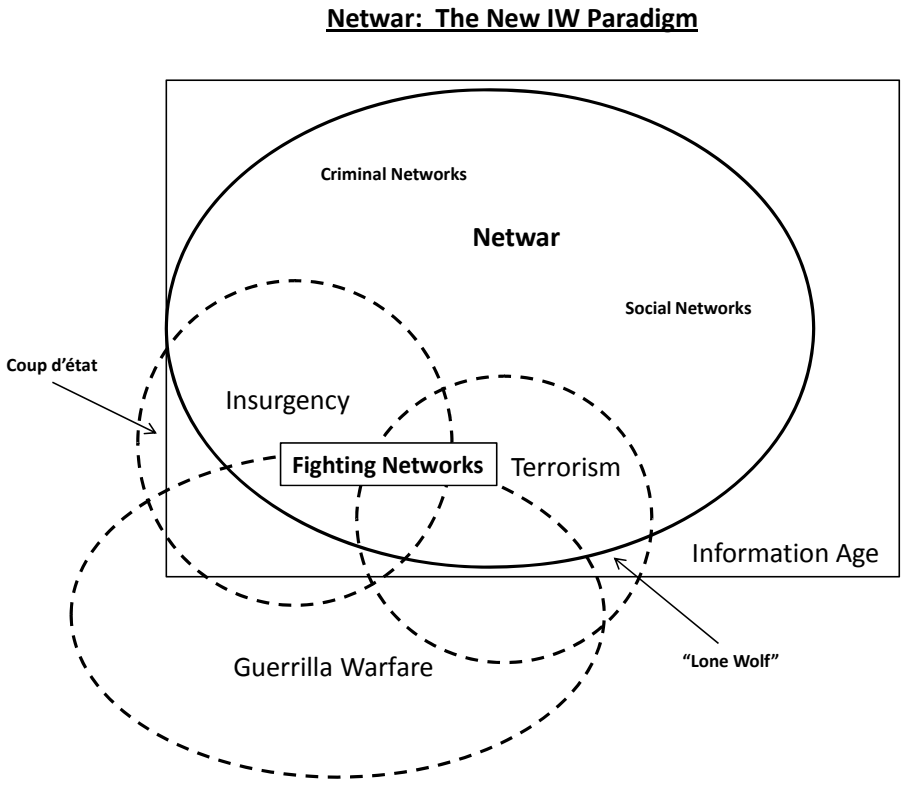

Figure 2. Netwar, the Warfighting Paradigm of the Information Age

[58] Thomas S. Kuhn, *The Structure of Scientific Revolutions* (Chicago: University of Chicago Press, 1962).

While the defining elements that characterize fighting networks stem from a combination of recent innovations and a synchronized style of warfare, some of their characteristics are recognizable throughout the history of irregular warfare. Irregular opponents have sought to confront and frustrate larger, professional armies from the earliest beginnings of organized warfare, and have done so using a variety of strategies and tactics. In his survey of irregular warfare, historian Lewis H. Gann stated, "the art of small wars is as old as the history of warfare itself."[59] These opponents are variously designated as partisans, guerrillas, insurgents, terrorists, and the like, and despite differences in origin, ideology, and aims, they have fought in similar ways. Generally out-numbered and facing a force disparity, these irregular opponents utilize concealment, sudden and shocking attacks, and sheer persistence to challenge professional armies. These commonalities have manifested themselves throughout the history of irregular warfare, and logically flow from the conditions of the conflict environment. "The technique of partisan warfare cannot be labeled either reactionary or progressive. It is based essentially on the precepts of common sense, and requires no particular mystique for its elucidation."[60] Perhaps because its principles are based on "common sense," it was not formally studied in the modern era until Colonel Le Miere de Corvey wrote his *Des partisans et des corps irreguliers*.[61] While irregular warfare received some attention from strategists, such as Clausewitz and Jomini, it was not viewed as a decisive form of warfare.[62] These studies relegated the idea of irregular warfare to a secondary technique, despite its extensive usage in wars of resistance; including those in America, Tyrol, Russia, and in Spain, where the term *guerrilla*, meaning little war, originated during the Spanish-Portuguese irregular resistance to French occupation from 1808–1813.[63] Resistance to colonial control formed the motivation for many of the small wars that

[59] Gann, *Guerrillas in History*, 78.

[60] Ibid.

[61] Chaliand, *Guerrilla Strategies*, 2.

[62] Ibid., 2.

[63] Asprey, *War in the Shadows*, xi.

marked the rest of this century.[64] By the 20th century, irregular warfare was a fairly common occurrence, especially in the twilight of the colonial era, but it was not until the middle of the 20th century, with the writings of Mao Tse Tung, that irregular warfare came to be seen as a systematic way to achieve political change.[65] Since that time, numerous antagonists have incorporated, or solely pursued, irregular warfare as a means to achieve their political end-state, most notably insurgents fighting wars of national liberation and modern terrorist groups. This history is significant because it reveals fundamental dynamics of irregular warfare, dynamics that lead to many of the ways in which networks fight and that produce strengths and weaknesses of these irregular opponents.

One of the primary characteristics of irregular struggles is the asymmetry in force between opponents. Irregular opponents are unable to oppose larger armies directly due to insufficient force, which is a combination of mass, firepower, and technical expertise. In addition, due to this disparity, if a professional army locates irregular opponents, they can be rapidly disrupted, if not eliminated. This lopsided result stems from the superior force advantage, and often, superior mobility that professional armies bring to bear.[66] The dynamic that results is one in which it is in the weaker opponent's best interest to remain undetected, or hidden, and where the stronger opponent seeks to find its "inferior" opponent. The fighting that does occur between these two sides hinges on the idea of relative combat power, where irregular forces seek to attack vulnerable points that present a favorable force ratio. Irregular opponents will use difficult terrain, urban, rural, and now the cyber realm, as well as the population, to provide concealment for their

[64] These small wars were so prevalent that colonial forces spent a great deal of time learning to confront irregular fighters throughout the globe. The summarized lessons learned may be found in Charles E. Callwell, *Small Wars: A Tactical Textbook for Imperial Soldiers* (1906) (Novato, CA: Presidio Press, 1990).

[65] Chaliand, *Guerrilla Strategies*, 7.

[66] This is not without exception as there are examples of professional forces routed or completely wiped out by irregular forces. Notable examples include the deceptive ambushes during the American Indian Wars, such as the Fetterman Massacre and the Battle of Little Big Horn, British confrontations during the Zulu Wars, and Afghan mujahedin battles against the Soviet Army. Modern intelligence collection technologies provide an additional challenge irregular networks face in confronting larger, professional armies, and examples of these larger ambushes are rarer in recent times. However, they are still very possible, as multiple battles in the 1st Chechen War, most notably the defense of Grozny, displayed.

activities. Complex terrain provides the concealment necessary to remain undetected, as well as to frustrate the generally superior mobility of the professionals. In addition, larger populated areas provide the means to blend in and often seek support from the population base. Those irregular opponents that seek the larger support of the population are generally called insurgents, and aim to wrest political control from an existing government. Insurgent networks operate with an information advantage, because they are able to conceal themselves, which provides a counter to their larger opponent's force advantage.[67] The terror tactics they employ, tactics that use many of the techniques of guerrilla warfare, properly define terrorist networks, which generally lack popular support for these tactics and have fewer ties to the larger population, and which requires more clandestine measures to be hidden. These characteristics are more in line with some modern irregular networks than guerrilla fighters are as they "do not function in the open as armed units, generally do not attempt to seize or hold territory, deliberately avoid engaging enemy military forces in combat and rarely exercise any direct control or sovereignty over either territory or population."[68] Overall, the ability of these irregular opponents to conceal themselves presents a counter to their opponent's force superiority, and creates the primary challenge of finding elements of these networks.

Within the realm of irregular warfare, fighting networks employ both guerrilla and terrorist tactics displayed by irregular fighters throughout time. Yet what makes a network's fighting characteristics revolutionary is the ability to fuse such techniques with innovations in organization and doctrine. This integration makes the network perspective crosscutting and a valuable characterization of irregular warfare, which provides insights into multiple types of irregular opponents. These characteristics provide such significance that their appearance dramatically changes irregular warfare, and has produced different attempts to characterize these changes. Martin van Creveld heralded this transformation, by stating, "in the future, war will not be waged by armies but by groups whom we today call terrorists, guerrillas, bandits, and robbers, but who will undoubtedly hit on more

[67] McCormick, "Diamond Insurgent/COIN Model," 6.

[68] Bruce Hoffman, "Defining Terrorism," in *Terrorism and Counter-Terrorism: Understanding the New Security Environment*, ed. Russell D. Howard and Reid L. Sawyer (Guilford, CT: McGraw-Hill, 2003), 22.

formal titles to describe themselves."[69] More recently, David Killcullen highlights this change by describing a "…tendency toward hybrid forms of warfare combining terrorism, insurgency, propaganda, and economic warfare to sidestep Western conventional capability…."[70] Hybrid warfare, or hybrid war, describes the fusion that results from networks employing irregular, conventional, and terrorist forms of conflict in a synthesized manner, a manner that poses a significant threat to the conventional armies of modern nation-states.[71] According to the 2007 U.S. National Maritime Strategy, "conflicts are increasingly characterized by a hybrid blend of traditional and irregular tactics, decentralized planning and execution, and non-state actors….using both simple and sophisticated technologies in innovative ways."[72] It is the fluid ability of networks to utilize a range of irregular tactics, while employing modern weapons systems, and harnessing the innovations of the information age that results in the hybrid nature of these conflicts. Displaying timeless characteristics, but heralding a revolution in warfare, networks are the primary threat to security and stability, and the ways in which they fight present considerable challenges for traditional war-fighting practices. Network style warfare provides a synthesized mode of fighting that revolutionizes, and, in many ways, transcends historical irregular warfare techniques.

B. A COMPARATIVE ANALYSIS OF WARFARE

Despite the revolutionary changes occurring in irregular warfare, it is common for dated terminology and generally descriptive language to be used to describe dramatically new threats. Significantly, the most advanced non-state actors today are still referenced using basic terms, such as guerrillas or terrorists, or even less descriptive terms, such as insurgents. While insurgents are accurately described as those fighting to change a governing authority, the term reveals little about the way in which they fight—its description is of a political nature. Much of irregular warfare is defined by insurgent

---

[69] Martin van Creveld, *The Transformation of War* (New York: The Free Press, 1991), 197.

[70] Kilcullen, *The Accidental Guerrilla*, 25.

[71] Hoffman, *Conflict in the 21st Century*, 8.

[72] Gen. James T. Conway, Adm Gary Roughead, and Adm Thad W. Allen, *A Cooperative Strategy for Maritime Security* (Washington, DC: Department of the Navy, 2007).

goals and terror tactics, but its characterizing style of fighting is guerrilla warfare. As previously described, guerrilla warfare generally speaks to irregular operations, and according to U.S. military doctrine, occurs in contested or occupied areas, and usually by indigenous people.[73] Since guerrilla warfare has served as the dominant descriptor of many revolutionary and insurgent struggles, it is often assumed it is synonymous with these efforts. However, while they both employ guerrilla warfare, the term itself is more accurately used generally to describe irregular opponents and the tactics they employ. Derived from, and representing "small wars," its descriptive power wanes in an era of globalization and flattening of technology.

In contrast, network-style warfare describes a method of fighting dramatically different from traditional warfare, and makes past descriptions of guerrilla warfare obsolete for defining today's unconventional networked threats. Netwar is a perspective that highlights the dramatic changes in conflict occurring in the information age and the rise and empowerment of networks as a form, which currently predominates across the spectrum of conflict.[74] Using the framework of organization, doctrine, operational methods, and information strategy, a comparative analysis of guerrilla warfare and violent netwar reveals their distinguishing elements, and highlights the revolutionary changes occurring in irregular warfare.

[73] U.S. Department of Defense, Joint Publication 3-05.01, *Joint Tactics, Techniques, and Procedures for Joint Special Operations Task Force Operations* (Washington, DC: U.S. Government Printing Office, 2007), GL–12.

[74] Arquilla and Ronfeldt, *The Advent of Netwar*, 7.

Forms of Warfare Displayed in an Irregular Warfare Environment				
	Organization	Doctrine	Operations	Info Strategy
Traditional Warfare	*Hierarchical *Mass Formations	*Primarily Offensive *Maneuver	*Firepower *Overwhelming Force	*Enemy Focused *Command & Control Centric
Guerrilla Warfare	*Hierarchical *Small Elements	*Inherently weaker *Protracted *Strategically Defensive	*Attrition *Hit and run *Deliberate *Safe-haven	*Local population
Network Warfare	*Decentralized *Nodes, or Cells *Autonomy *Multiple Linkages	*Swarming *Blurs Offense & Defense	*Synchronized Attacks *Decisive Engagements *Pulsing	*Information Drives Operations *Information Diffusion

Table 2. A Comparative Look at Forms of Warfare Existing in the Irregular Warfare Domain.

Organizationally, guerrilla warfare and netwar both feature small elements, but beyond this, their similarities end. Guerrilla warfare tends to organize small elements in a hierarchical manner, with traditional ideas of command and control. Authority is pushed down the chain in a vertical manner, and uses cellular structures and security measures in an attempt to conceal this hierarchical structure. While networks are composed of nodes, the formation of linkages between these nodes, and the manner in which they form clearly distinguish netwar from guerrilla warfare. The small nodes in netwar are robustly linked in various structural combinations, but trend towards all-channel formation, with multiple linkages forming a robust network form.

Doctrinally, guerrilla warfare centers on the strategic defensive and aims to build up forces to confront a superior opponent. Since guerrillas are inherently weaker, they are limited to hit-and-run tactics, and are focused more on disrupting than on defeating an opponent. The goal of this disruption is to wear out the enemy opponent over time, leading to the protracted nature of guerrilla warfare. Netwar, in contrast, blurs

distinctions of offensive and defense and describes more fluidity in operations. The hallmark doctrine of network-style warfare is swarming, which involves self-synchronized nodes or cells able to attack *en masse*.

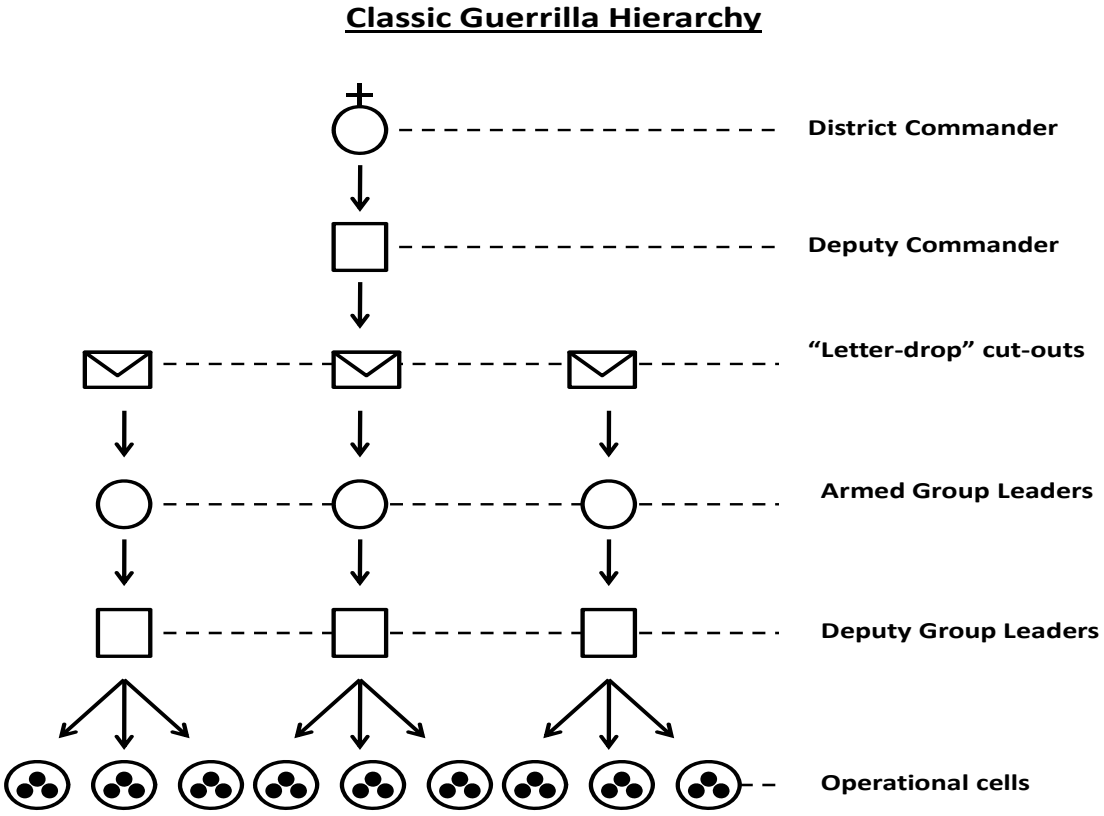

Figure 3. A Classic Guerrilla Structure with Hierarchical Organization[75]

Operationally, guerrilla warfare is focused on deliberate attacks that seek to attrite an enemy's will over time. This attrition is focused on attacks, which are designed to disrupt an opponent's military efforts, but more importantly, convince the population of the guerrilla's stronger will. Guerrillas operate deliberately, and require intelligence to achieve surprise. Further, their tactics are based on a concept of hit-and-run attacks, which generally have little decisive effect. Fundamentally weaker, guerrillas also require

[75] This graphic depicts the Algerian National Liberation Army structure as depicted in Trinquier, *Modern Warfare: A French View of Counterinsurgency*, 10.

a safe-haven to recover and reorganize. Netwar focuses on fluid attacks that seek a decisive effect. Often, networks attack in a pulsing manner with cycles of information collection and analysis, then decisive attacks. Networks may benefit from the inaccessibility that physical terrain provides, but the networked form allows them to achieve concealment in ways that reduces the need for a purely physical safe haven.

The information strategy employed by guerrillas attempts to achieve control over popular opinion at the local level, which is generally accomplished by attempting to gain commitment to a cause. Networks understand the dynamics of the information age and seek to dominate information strategy throughout the conflict. Networks go beyond such elusive goals as winning hearts and minds, and use information as a powerful lever against their opponents. The narrative dimension of netwar describes the information aspect, which provides an overarching concept and unifies disparate and dispersed nodes. In fact, netwar as a whole tends to place more emphasis on information strategy than it does on actual conflict.

Netwar and guerrilla warfare are dramatically different at the organizational and doctrinal levels, and networks seem to be leading in information strategy innovations across all types of warfare. At the tactical level, some similarities exist, as networks still functions as small elements, or nodes, and utilize aspects of small unit tactics, such as the raid and ambush. The notable guerrilla Colonel Russell Volkmann, who conducted stay-behind actions against Japanese forces in the Philippines, presciently stated, "a future war, waged with highly mobile forces, supported by scientific and mechanical means of tremendous destructive potential, will lead to a greater dispersion of forces, fluid battle-fronts, and widespread isolated action—a setting ideal for guerrilla warfare."[76] While Volkmann foresaw changes in irregular warfare, the dramatic changes resulting in the rise of network style warfare, have far surpassed expectation. While "network warfare looks a lot like guerrilla warfare with incredibly powerful weapons," its characteristics make it truly unique, and a "…new significant step…" in warfare.[77] Networks display

[76] Russell W. Volckmann, Col., *We Remained* (New York: W.W. Norton Co., 1954), 237.

[77] Bruce Berkowitz, *The New Face of War: How War Will be Fought in the 21st Century* (New York: The Free Press, 2003), 17.

these characteristics with a fluidity that highlights their ability to synchronize multiple tactics, integrate modern technology, and leverage modern war-fighting concepts, such as the use of combined arms and sensors. The comparison of these modes of conflict displays the dramatic changes in irregular warfare, and the unique suitability of the netwar perspective in defining and understanding these changes.

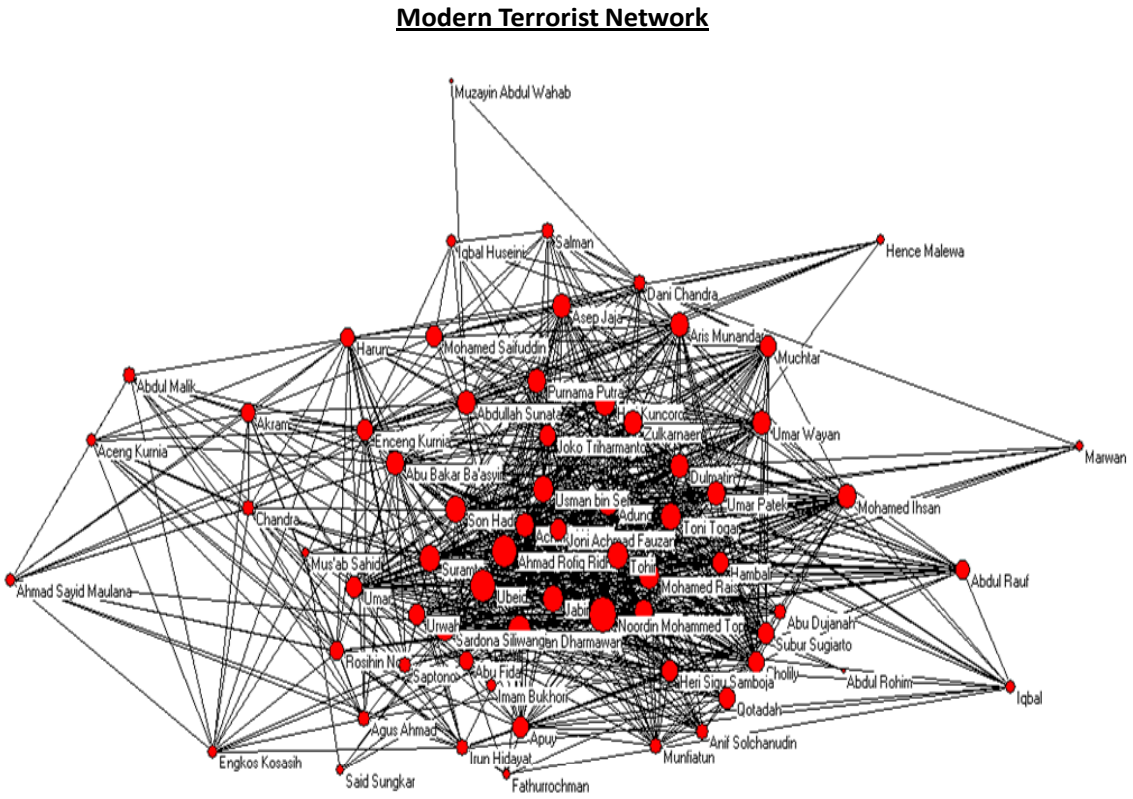

Figure 4. The Noordin Mohammed Top Terrorist Network[78]

[78] This sociogram depicts the members of the Noordin Top Terrorist Network who were "alive and free" at the time of the data collection. The data is from International Crisis Group, "Terrorism in Indonesia: Noordin's Networks," *Asia Report #114*, (Brussels, Belgium: International Crisis Group, 2006), http://www.crisisgroup.org/en/regions/asia/south-east-asia/indonesia/114-terrorism-in-indonesia-noordins-networks.aspx. Data structured and analyzed by Defense Analysis students in the course "Tracking and Disrupting Dark Networks," under the direction of Professor Nancy Roberts, Co-Director of the CORE Lab, and updated by Dr. Sean Everton.

C. NETWORK ANALYSIS

Network terminology describes numerous elements and structural forms, and its use is increasingly prevalent with a growing awareness of network properties. At their most basic level, networks are composed of two primary elements, nodes, or actors; and the linkages, or ties that connect these nodes.[79] Given these basic structural attributes, networks are ever present, and the term defines combinations in the physical realm, such as telephone networks, and in the social realm, such as interpersonal networks—leading to the term "networking." In general, it is used to describe social organizations composed of more informal linkages, and is now a common appendage to describe irregular opponents, such as terrorist networks, insurgent networks, and narco-trafficking networks. These networks have elements that form deliberately, but also in many cases, utilize the normal networking that people conduct on an informal, ad-hoc basis. As non-state actors become increasingly prevalent, and empowered by modern information technology, networks are formed by virtue of the informal relationships that exist among those joining. These networks are fluid in composition and their informal nature differentiates them from more established organizations, such as the hierarchical structures that define nation states, or large business organizations. This section of the thesis examines characteristics of violent, illicit networks in irregular warfare and seeks to understand the ways in which they fight, as well as provide a framework of strengths and weaknesses, that is both historically informed, and incorporates the latest innovations in unconventional tactics and techniques. Bruce Berkowitz describes these networks' fluid nature and their essential features:

> Fighting networks can be as small as a three-man terrorist organization or as large as a joint task force. They can operate on the scale of a few city blocks or an entire hemisphere. The can use cheap, simple handheld weapons or weapons that cost hundreds of millions of dollars. Their essential feature lies in how they use information technology and how they operate.[80]

---

[79] Newman, Barabási, and Watts, ed., *The Structure and Dynamics of Networks*, 2.

[80] Berkowitz, *The New Face of War*, 17.

Fighting networks in irregular war operate violently outside the legal constraints of nation states, and conduct illegal activities ranging from criminal enterprise, insurgency, and terrorist activities, usually in a combination of various activities and ways. A common description of network threats is "dark networks," a reference to the "covert and illegal" nature of illicit networks.[81] The "dark-side" of networks originally referred to violent networks to differentiate them from social networks, which is a useful distinction that focuses on their violent behavior.[82] It has since been expanded to include the difficulties of identifying and locating irregular opponents, but in this sense, it may be overemphasized, because those tasked with such activities, may see more of a network structure than is commonly understood. Most importantly, networks in irregular warfare have both "dark" and "light" aspects, and one of their fundamental challenges is the push-pull between the need to maintain clandestine elements required for secrecy, and the need to conduct essential overt activities, such as generate resources, recruit, conduct operational activity, and influence popular opinion.

Fighting networks have elements of clandestine structure, but also elements of open connectivity. The clandestine attributes of networks derive from concealment and their compartmentalized attributes, which preserve the organization's existence. The traditional, tightly controlled, and hierarchical models of insurgent and terrorist activity call for a cellular structure built off recruitment in a hierarchical manner. However, these organizations require a high degree of control, intensive security measures in the form of cut-outs, and excessive redundancy. Models that depict a formal, structured underground that is highly cellular and compartmentalized place excessive emphasis on these features; features which discourage autonomy, flexibility, and innovation.[83] While some aspects of

[81] Raab and Milward, "Dark Networks as Problems," 415. According to most intelligence definitions and military doctrine, the term covert implies that the actor is deniable, while the word clandestine describes activity that is hidden. In view of these distinctions, networks are more accurately described as clandestine in nature.

[82] Arquilla and Ronfeldt, *Networks and Netwars*, 9.

[83] An example of this emphasis is the School of Advanced Military Studies monograph, MAJ Derek Jones, *Understanding the Form, Function, and Logic of Clandestine Cellular Networks: The First Step in Effective Counternetwork Operations* (U.S. Army Command and General Staff College, 2009). The excellent description of classic clandestine structure in this work fails to account for the pressures that make these idealized forms less realistic.

terrorist and insurgent networks manage to maintain a clandestine, cellular structure, the costs involved include limited operational activity, tight control, and restricted communication. The reality of networks is that attempts are made to maintain clandestine control, mostly within the leadership structure, but that deliberate compromises are often made to keep the network functioning and operationally viable. Networks are far more decentralized, fluid, and open, balancing these attributes with some elements of structural control; where control is required for planning, operations, or to preserve leadership structure. These reasons prompted the noted al-Qaeda strategist Abu Musab al-Suri to reject such "secret—regional—hierarchical," models in favor of the "open fronts, …methods of individual jihadi operational activity, [and] the methods of total resistance," which reflects this network's transition to a netwar orientation.[84]

Networks have both strengths and weaknesses, and while much of the literature emphasizes the advantages of the networked form, understanding a networked opponent's weaknesses is critical in the brutal conflicts of irregular warfare. While some network studies draw primarily on business models that emphasize the advantages of the horizontal collaboration displayed by networks in the short product life cycles and rapid technological changes of the global economy, it is imperative also to incorporate the unique set of constraints, or pressures, that networks face.[85] Existence as a clandestine organization involves high risk and pressure from hostile, external forces, which produces a set of influences that impact the effectiveness of the network form.[86] Understanding the impact of these pressures provides a critical aspect of understanding the strengths and weaknesses of networks in the dynamic and hostile environment of irregular warfare. In addition, the distinction between networks and hierarchies from a

---

[84] Abu Musab al-Suri, "The Global Islamic Resistance Call," in *Architect of Global Jihad: The Life of Al-Qaeda Strategist Abu Mus'ab al-Suri*, ed. Brynjar Lia (New York: Columbia University Press, 2008), 367.

[85] Mette Eilstrup-Sangiovanni and Calvert Jones, "Assessing the Dangers of Illicit Networks: Why Al-Qaida May Be Less Threatening Than Many Think," *International Security* 33, no. 2 (Fall 2008): 11.

[86] See, for example, Bonnie H. Erickson, "Secret Societies and Social Structure," *Social Forces* 60, no. 1 (1981): 195. http://www.jstor.org/stable/2577940; J. Bowyer Bell, "Aspects of the Dragonworld: Covert Communication and the Rebel Ecosystem," *International Journal of Intelligence and Counterintelligence* 3, no. 1 (1989): 15–43, 23; J. Bowyer Bell, "Revolutionary Dynamics: The Inherent Inefficiency of the Underground," *Terrorism and Political Violence* 2, no. 2 (Summer 1990): 193–211.

strictly organizational perspective limits and ignores the synchronized nature of network-style warfare. While organizational structure provides a significant aspect, studies that only examine networked-based threats on this basis incompletely assess the full range of strengths and weaknesses that a synthesized system of network-style warfare provides.[87]

To understand the threats from today's fighting networks, this study begins with a detailed analysis that combines principles of irregular warfare with insights from network theory and examines the impact of modern information technology. The principles of irregular warfare derive from the historical record and modern usage, and represent tactics and techniques used by insurgent and terrorist networks, as well as unique aspects displayed by modern networked opponents. While many aspects of truly revolutionary fighting networks exist, and reflect the current dynamic of the information age, this is not to suggest that previous studies of irregular warfare are obsolete. An analysis of multiple bodies of knowledge provides the foundation for generating characteristics, which offers a combined understanding of how networks fight. For the scope of this study, networks in irregular warfare exhibit characteristics defined by their organizational attributes, doctrine, operational methods, and information strategy. These "lenses" provide an overall perspective, which produces specific characteristics. Each of these characteristics adds to the understanding of networks and describes ways in which they fight. Other frames of analysis include the narrative and social dimensions, both critical elements in forming and uniting networks, and essential parts of a comprehensive view of networks.[88] In this study, relevant elements of the narrative and social dimensions are examined through the lenses of organizational attributes and information strategy, to

[87] For examples of this organizational focus, and an examination of structural strengths and weaknesses, see Eilstrup-Sangiovanni and Jones, "Assessing the Dangers of Illicit Networks;" Tucker, "Terrorism, Networks, and Strategy," 2. An article which examines the nature of Al-Qaeda's core cadre is Rohan Gunaratana and Aviv Oreg, "Al-Qaeda's Organizational Structure and its Evolution," *Studies in Conflict & Terrorism* 33, no. 12 (2010): 1043–1078, http://dx.doi.org/10.1080/1057610X.2010.523860. An article which examines the blend of hierarchy and network forms in terrorist organizations is Shaul Mishal and Maoz Rosenthal, "Al-Qaeda as a Dune Organization: Toward a Typology of Islamic Terrorist Organizations," *Studies in Conflict & Terrorism* 28, no. 4 (2005): 275–293, http://dx.doi.org/10.1080/10576100590950165.

[88] Arquilla and Ronfeldt, *Networks and Netwars*, 324.

provide a succinct picture of how networks fight. These characteristics are then examined to provide a summary of the strengths and weaknesses exhibited in the ways networks fight.

1. Organizational Perspectives

Networks are organizations socially derived from a composition of actors and linkages. These basic foundations are no different than any other organization, which are "groups of people working together to achieve some common purpose," that facilitate the ability to "accomplish more than we could ever do alone."[89] The distinct structural characteristics of networks are "limited central control, local autonomy and informal, flexible interaction based on direct, personal relations…."[90] Most of the study of organizations is derived from organizational theory, but this study incorporates social network analysis and traditional cultural forms to provide a comprehensive description of the organizational characteristics of networks. Organizational design is the defining level of network analysis, and a network's structure provides the basis for other war-fighting aspects.[91] In most ways, organizational characteristics are generally similar across both violent networks and their more socially acceptable counterparts, an aspect which speaks to the applicability of the netwar concept and reinforces the importance of network-based organizations.

a. Organizational Theory

Organizational theory holds that differences exist in attributes among organizations, and these distinctions are significant enough that they influence an organization's performance. These differences have a pronounced effect in the dynamic, high-risk environment of irregular warfare. Many of the fundamentals of organizational theory stem from the assumptions of the Machine Age, and hold that an "organization is like a machine: a collection of parts that need to be standardized and centrally

---

[89] David P. Hanna, *Designing Organizations for High Performance* (New York: Addison-Wesley Publishing, Co., 1988), 1.

[90] Eilstrup-Sangiovanni and Jones, "Assessing the Dangers of Illicit Networks," 18.

[91] Arquilla and Ronfeldt, *Networks and Netwars*, xi.

controlled."[92] However, it is now commonly understood that an organization is more like a system, where the relationships of all the pieces and their total interaction are what is important. These recent ideas portray organizations as a combination of interrelated parts that interact with its environment, such as the organization's purpose/goals, inputs, tasks, and output. The idea of an organization as a system that functions in relation to its environment led to the idea that no fixed ideal organizational form exists, but that organizational effectiveness is contingent on various aspects of the environment. This belief is the core of organizational contingency theory, which provides considerable insight into the study of networks, and aids in understanding that the modern irregular warfare environment requires certain forms.[93]

From an organizational perspective, hierarchies provide a structure that dispenses authority, material resources, and ideology in a vertical manner.[94] In a hierarchy, particularly one based on machine-type bureaucracy, complex tasks are broken down into specific jobs to achieve greater efficiency. However, this organizational type may limit communication outside of specific divisional or functional areas, "thus, a hierarchical mode of thinking tends to ignore the potential and real influence of formal and informal ties among actors that cut across social categories and group boundaries. It also ignores other forms of everyday social relations that affect actors' identities, attitudes and behavior."[95] Organizationally, networks allow for a greater degree of connectivity and are more resilient to disruption. Arquilla and Ronfeldt define a network as a "set of diverse, dispersed nodes that share a set of ideas and interests and are arrayed to act in a fully internetted 'all-channel' manner."[96]

---

[92] Hanna, *Designing Organizations for High Performance*, 4.

[93] Organizational theorists that contributed to contingency theory include John Woodward, Paul Lawrence, and Jay Lorsch, but it is Henry Mintzberg's synthesis of ideas in *The Structuring of Organizations* (1979) that provides the most comprehensive framework.

[94] Gunaratana and Oreg, "Al-Qaeda's Organizational Structure and its Evolution," 1045.

[95] Mishal and Rosenthal, "Al-Qaeda as a Dune Organization: Toward a Typology of Islamic Terrorist Organizations," 277.

[96] Arquilla and Ronfeldt, *Networks and Netwars*, 7.

b. Social Network Analysis

Social network analysis holds that all combinations of social linkages are networks regardless of hierarchical or decentralized attributes.[97] Using the social network analysis method, even the most formal hierarchical structure is technically a network; it is just organized with specific attributes. Social network analysis describes these attributes as variations in network typography. Some of the basic assumptions of social network analysis include the following.

- Actors and their related actions are interdependent with other actors
- Ties between actors are seen as channels for the transfer or flow of various types of resources
- Social structures are seen in terms of enduring patterns of ties between actors
- An actor's position in the social structure impacts its beliefs, norms and observed behavior
- Social networks are dynamic entities that change as actors, subgroups, and ties between actors enter or leave the network[98]

Social network analysis may be applied on the macro level, examining groups of people, organizations, and even countries, or at the micro level, addressing individual actors and their connections. These social structures are a "network of social ties," which "transmit behavior, attitudes, information, or goods."[99] While the structural framework is important, what moves between the linkages is also important in social network analysis.

Measures of network topography include metrics for an entire network, individual actors, and those that measure the flow of resources within a network. For example, the network density measures the total number of ties within a network divided by the total possible number of ties, which provides a picture of how many of the

---

[97] Ronald L. Berger, "The Analysis of Social Networks," in *Handbook of Data Analysis*, ed. Melissa Hardy and Alan Byman (London: SAGE Publications, 2004), 505.

[98] This is a slightly abbreviated list of assumptions from those compiled and listed by Sean Everton. Sean Everton, *Tracking Destabilizing and Disrupting Dark Networks with Social Network Analysis* (Master's thesis, Monterey, CA: Naval Postgraduate School, 2009), 17.

[99] Wouter de Nooy, Andrej Mrvar, and Vladimir Batagelj, *Exploratory Social Network Analysis with Pajek* (New York: Cambridge University Press, 2008), 3.

potential linkages between actors are utilized. Network density is positively related to a stronger following of accepted norms and behavior within the social network.[100] Individual actor measurements include measures of centrality, which seeks to determine the position of an actor in the network based on the assumption, that because of their position, they "often enjoy better access to information and better opportunities to spread information."[101] Social network analysis metrics apply to the most hierarchical organizations, with rigid, formal linkages, and to the most informal organizations, with little to no organized structure.

Two main types of network formation exist, random and free-scale. Random networks are more theoretical and static and scale-free networks exhibit the "real-world" characteristics of growth and preferential attachment. One of the oldest forms of network models, the random graph, displays random networks but this graph has a scale, defined by a normal distribution around an average node.[102] Scale-free networks, in contrast, have a power-law degree distribution, or long-tail graph, which reflects that in most actual networks a small number of nodes are more connected than the rest.[103] Growth reflects the dynamic nature of real-world networks, while preferential attachments describes the phenomena that nodes prefer to attach to more connected nodes.[104] The majority of data-based studies suggest that most social networks have free-scale characteristics, and it may be a universal characteristic of many networks.[105]

---

[100] Everton, *Tracking Destabilizing and Disrupting Dark Networks with Social Network Analysis*, 14.

[101] Ibid.

[102] Newman, Barabási, and Watt, ed., *The Structure and Dynamics of Networks*, 232.

[103] Barabási, *Linked*, 70–71.

[104] Ibid., 87.

[105] Newman, Barabási, and Watt, ed., *The Structure and Dynamics of Networks*, 335–336.

Random vs. Scale Free Networks

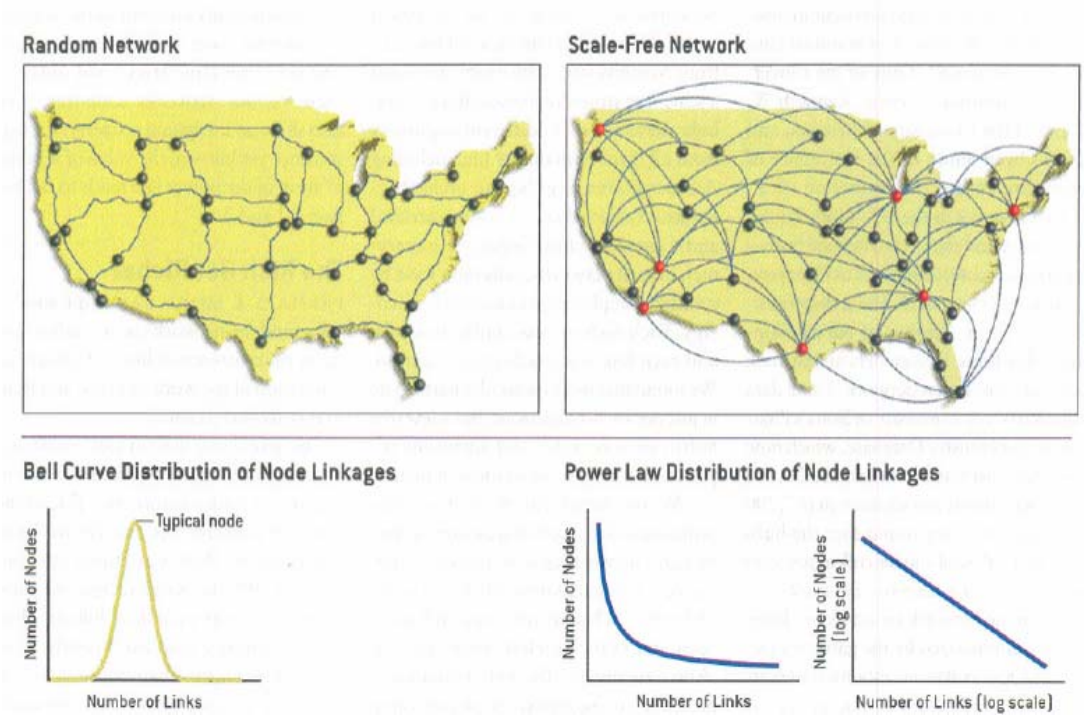

Figure 5. Differences in the Distribution of Random and Scale-Free Networks[106]

Network theory provides a basis for three general topologies, which are used in social network analysis and most descriptions of network activity. According to Arquilla and Ronfeldt, there may be combinations and variations of these three types, but the basic topologies are the following.

- Chain—the network resembles a linear fashion, where contacts are separated from each other in an end-to-end fashion, and people, goods and services move through intermediate nodes in sequential fashion.
- Star, or Hub—in this network form nodes are linked to a central node in a hub and spoke configuration and resources and communication must flow through the central hub.

[106] Albert-László Barabási and Eric Bonabeau, "Scale Free Networks," *Scientific America* 288, no. 5 (May 2003): 50–59, http://www.nd.edu/~networks/Publication%20Categories/01%20Review%20Articles/ScaleFree_Scientific%20Ameri%20288,%2060-69%20(2003).pdf.

- All-Channel—the network forms in a matrix of connections with every node connected to each other node in a dense fashion.[107]

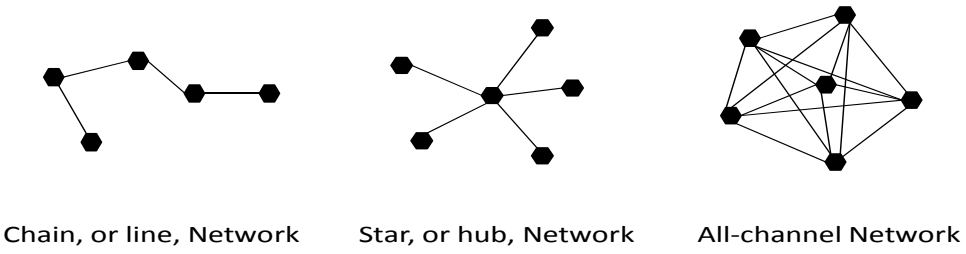

Figure 6. Three Basic Forms of Network Structure

c. Cultural Forms

Networks are dynamic and while it is clear that network theory provides a fundamental mode of analysis, multiple paradigms provide greater perspective. Ronfeldt provides one such viewpoint by describing the al-Qaeda organization as a "classic tribe, one that wages segmental warfare."[108] This idea of a tribal organizational structure provides another viewpoint on network organization, one that "…overlaps with the network view, but has its own implications."[109] The tribal paradigm is a cultural form that emphasizes kinship and religion in organizational constructs that are egalitarian, segmental, and acephalous, or lacking formal leadership.[110] While standard works on modernization and development assessed tribal and clan structures as archaic and having fading relevance, in many societies they remain, and greatly enhance social

[107] Arquilla and Ronfeldt, *The Advent of Netwar*, 49. Numerous other publications reference the same basic types first proposed in this manner by Arquilla and Ronfeldt.

[108] David Ronfeldt, "Al-Qaeda and its Affiliates: A Global Tribe Waging Segmental Warfare," in *Information Strategy and Warfare: A Guide to Theory and Practice*, ed. John Arquilla and Douglas A. Borer (New York: Routledge, 2007), 1–15, 35.

[109] Ibid., 35.

[110] Ibid., 37–38.

connectivity.[111] Kinship is the formative factor in tribes and family ties build into groupings usually designated as clans. Multiple clans who share similar cultural values and religious beliefs loosely organize into tribes, coalescing through similar ideology, but achieving cohesion and structure through their kinship-based tribal groupings. According to Ronfeldt, "…kin and their associates operate on lateral as much as vertical ties…," making for "….highly flexible social possibilities that resemble not only circles within circles but also circles across circles."[112] These organizational structures stem from the nature of classic tribal principles. The first principle is that classic tribes are egalitarian, meaning that there is a high degree of respect for individual autonomy. This promotes an ethos that limits hierarchical tendencies, and promotes leadership that is "…modest, generous, self-effacing and treat[s] others as peers."[113] The basis behind the segmental principles is that each tribe is more or less similar, and there is no real specialization, or from an organizational theory perspective, differentiated. This provides for structures that are able to have high degrees of fusion and fission, uniting and separating with a remarkable fluidity. The third principle is that classic tribes are acephalous. Those who were in positions of authority, such as a chief, had influence as a broker or advisor, but decision making was based on deliberation and consensus, usually in the form of open tribal councils. These insights from cultural forms are particularly valuable in describing fighting networks formed from social networks within a culture that emphasizes tribal characteristics. As Richard Schultz states, "one of the more disturbing trends of non-state armed groups is the extent to which such groups, including these clan-based groups, are cooperating and collaborating with each other in networks that span national borders and include fellow tribal groups, criminal groups, and corrupt political elements."[114]

---

[111] Richard H. Shultz and Andrea J. Dew, *Insurgents, Terrorists, and Militias: The Warriors of Contemporary Combat* (New York: Columbia University Press, 2006), 41–42.

[112] Ronfeldt, "Al-Qaeda and its Affiliates," 37.

[113] Ibid., 38.

[114] Shcultz and Dew, *Insurgents, Terrorists, and Militias*, 53.

2. Organizational Attributes

Each of these organizational perspectives provides insights into the organizational factors operative in networks. While there is analytical value in describing every social construct through a lens of social network analysis, for the purpose of this study, networks are organizations that emphasize the following attributes of decentralization, greater autonomy, informal chains of authority, and dispersed communications flow, and this separates them from organizations commonly characterized as hierarchies. The application of contingency theory to the study of networks is a developing field, as most network analysis is derived from elements of network theory, but the combination of the two perspectives provides for a richer understanding of networked organizations. The tribal form also provides valuable insight into understanding the formative ties within networks, and the norms that emphasize segmented activity. The following organizational characteristics are essential elements in understanding how networks fight.

a. Decentralization

Networks are structurally characterized by high levels of decentralization, which allows for autonomous action and high degrees of operational initiative. Organizational structures are generally configured to the nature of their task, and must be to achieve any degree of efficiency. Organizations faced with routine tasks and simple communications prefer a centralized structure, but organizations that must face complex tasks and a high degree of information transfer decentralize to achieve greater efficiency.[115] Decentralization refers to an element of structure that captures the degree of autonomy at all levels of the network. In addition, decentralization provides a means to describe authority within an organization, and in most networks, in irregular warfare, a distribution of authority exists. However, although authority flows vertically, there is much less control and direction, in the form of orders and plans, than in most organizations. This combination of vertical authority, but less directive control enables sub-elements of the network to remain flexible based on the conditions they face.

[115] Jeffrey Pfeffer, *Locations in the Communications Network* (Boston: Harvard Business School Press, 1994), 114.

Organizational theory postulates two ways to achieve decentralization of authority, vertically and horizontally. Vertical decentralization describes delegation of power down a vertical chain of authority, while horizontal decentralization describes the distribution of power out away from a vertical chain.[116] Networks achieve their best fit to the environment and their goals using a combination of these aspects of decentralization. Further, the pressure placed against networks in response to their illegal, violent activity, is a significant factor in producing a complex environment. "Because of external pressure, global guerrillas have atomized into loose, decentralized networks that are more robust and learn more quickly than traditional hierarchies."[117]

Information technology allows networks to decentralize further, as they substitute information flows via technology for what previously may have required a more hierarchical structure.[118] These advantages, combined with the tendency of networks to grow increasingly dense to maintain strong affiliations in dangerous circumstances, produce conditions that favor decentralization over centralized hierarchical control. The greater decentralization, which characterizes networks, creates more autonomy and freedom of action, especially in all-channel networks. In fact, networks achieve much of their effectiveness because greater autonomy at the individual actor level allows for faster decision making.[119] This freedom of action is a hallmark of small-unit maneuver throughout warfare, and it allows these small units to exert tremendous operational initiative. Since these units are able to act independent of a centralized control system, they are able to take the initiative at the tactical level. Even in conventional, hierarchical military commands, local initiative usually determines success on the battlefield, and it is a hallmark of tactical advantage. Numerous instances of junior leaders taking the initiative, even when outside their direct responsibility, have proved the

---

[116] Henry Mintzberg, "Organizational Design, Fashion or Fit?," *Harvard Business Review* (January–February 1981, reprint 81106), 5.

[117] Robb, *Brave New War*, 15.

[118] Lee G. Bolman and Terrence E. Deal, *Modern Approaches to Understanding and Managing Organizations* (San Francisco, CA: Jossey-Bass, 1984).

[119] Tucker, "Terrorism, Networks and Strategy," 4.

value of initiative in determining the outcome of battle.[120] This is certainly true in irregular warfare, where much of the conflict occurs at the local, tactical level, and where rapidly changing conditions require swift responses independent of a formal order, or planning process. In fact, initiative at the nodal level provides the capacity to execute fluid swarming attacks.

b. Synchronized Nodes

Networks fight with nodes or cells, small elements that provide advantages in tactical control and security. Although networks are generally smaller than their opponents, as in the case of a non-state actor confronting a modern military, this is not always the case, and the asymmetry between opponents is due to differences in force. Mass is rarely a factor in irregular warfare engagements, and dispersion provides a better measure of force arrays. For this reason, smaller nodes provide multiple advantages to networks, including ease of tactical control and greater security.[121] These smaller groups require less direction and control to maneuver, and can achieve greater autonomy because they do not require complex direction. Yet, the same attributes that make nodes easy to control at the tactical level provide challenges in mass coordination of multiple elements. Paget highlights these challenges when writing about irregular forces in the mid-20th century, "This system of small groups is forced on the insurgents by their need for dispersion and mobility, and it suffers from the resultant weakness that effective control and good communications are both difficult to maintain."[122] However, information technology provides modern fighting networks with the ability to synchronize their efforts and communications more effectively while maintaining small, decentralized elements. Unlike traditional irregular opponents, networks allow greater communications, and their fundamental building blocks of nodes and cells are linked and empowered by a high-degree of connectivity.

---

[120] S. L. A. Marshall, *Men Against Fire: The Problem of Battle Command in Future Wars* (Alexandria, VA: Byrrd Enterprises, Inc., 1961), 61.

[121] Sean J. A. Edwards, *Swarming and the Future of Warfare* (Santa Monica, CA: RAND, 2005), 93.

[122] Julian Paget, *Counter-Insurgency Operations: Techniques of Guerrilla Warfare* (New York: Walker and. Company, 1967), 22.

Finally, nodes also provide for greater security, by compartmenting throughout the network, and by facilitating evasion. By ensuring small, segregated groups, a network is able to restrict information flow when necessary. "Security is always a problem to the insurgents who have to guard constantly against subversion, informers, traitors and deserters. Their security is always of the highest standard, and vital information is protected by adopting the 'cell' system, whereby only one person in each group knows the details and future plans and can identify his next superiors and juniors."[123] The cellular system is composed of small groups with strong ties, which provide some advantages in ensuring that segregation exists between cells, but with obvious downsides once, the cell itself is compromised. Operationally, smaller elements provide networks the means to disperse, and aid in remaining un-detected. Large groups of personnel are easily identified through visual means, and face greater difficulties achieving stealth during evasion.

c. Resiliency

Irregular warfare is dynamic and networks achieve resiliency through organizational structures with multiple linkages. According to network theory, random weak links provide resilient strength in network structure. Mark Granovetter, in his highly influential paper, "The Strength of Weak Ties," established that the crucial links in overall network formation are the weak links between actors.[124] This is somewhat counter-intuitive because it is natural to assume that strong ties would be the most effective bridges that tie various elements of networks together. However, weak links actually provide the "…social shortcuts, that if eliminated, would cause the network to fall to pieces."[125] Weak ties provide a high degree of resiliency because they allow a network to form bridges even when the strong ties are severed (strong ties usually characterize the most active parts of the network, and hence, the once most subjected to pressure and change).

---

[123] Paget, *Counter-Insurgency Operations*, 22.

[124] Granovetter, "The Strength of Weak Ties," 78, 1360–1380.

[125] Buchannan, *Nexus*, 43.

This structural property works in conjunction with the role of hubs, which are actors with a high degree of connections to other actors. Hubs ensure that networks remain connected and resilient in a way that redundancy alone cannot achieve. "The hubs act as a kind of glue within the network. Since an uncoordinated attack targets elements at random, it almost always knocks out unimportant elements with few links, while missing the hubs. In this way, the small-world architecture makes a network resilient against random failure or unsophisticated attack."[126] Further, networks utilize hybrid forms of chain, star, and all-channel structures in sophisticated combinations, which increase task efficiency and aid in overall network resiliency.

From an organizational theory perspective, resiliency is often (but not only) explained through redundancy. If one actor or system were to be removed from the organization, there would be another waiting to replace it. Yet, networks must balance their ability to control with the costs imposed by additional organizational structure, and a high-level of redundancy imposes costs in flexibility, resources, and coordination. Networks remarkable persistence in irregular warfare shows that, "…decentralized structures are more resilient than centralized ones because the violation of the integrity of any one of their branches has little effect on the ability of other branches to function and because their leaders are less useful to target."[127]

d. Flexibility

Effective networks are flexible, adapting their structure to the environmental conditions, which makes them resistant to any one form of pressure. Networks must be able to react to the pressures they face, and return to an equilibrium state based on their goals and environment. Inflexible networks will be unable to adjust to changes in the environment, fail to react to pressure, and incur higher operational risks. An optimal structure exists where networks are neither too strong and redundant, nor are ties too weak and loose. Social network analysis distinguishes between these two sets of characteristics with the terms "provincial," as in "confined to the provincial news and

[126] Buchannan, *Nexus*, 132.

[127] Sinno, *Organizations at War in Afghanistan and Beyond*, 77.

view of their close friends," or "cosmopolitan," meaning open exchanges between many loose acquaintances [128] Networks under extreme pressure are generally loosely organized, and less able to mobilize for operational activity. Networks that find themselves in a provincial state, with close, strong ties may be more operationally effective, but also more isolated. In either situation, networks exhibit flexibility by adjusting to the environmental pressures to maintain an effective balance.

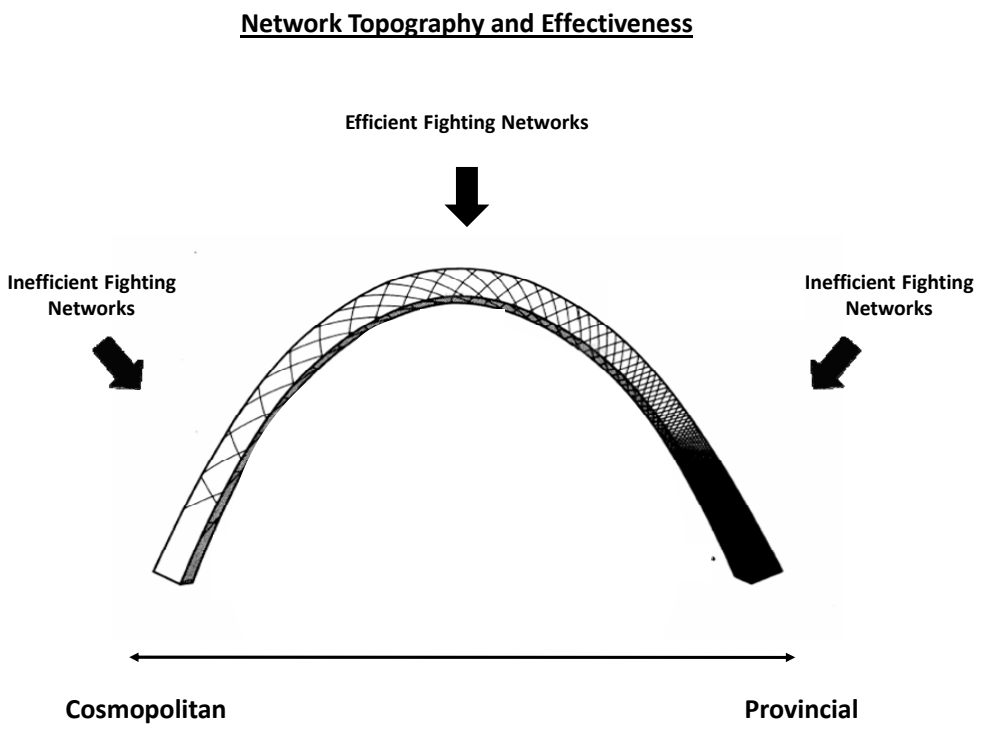

Figure 7. Efficient Network Structure[129]

[128] Granovetter, "The Strength of Weak Ties," 78, 1360–1380, Everton, *Tracking Destabilizing and Disrupting Dark Networks with Social Network Analysis*, 180.

[129] Figure originally depicted in Bernice A. Pescosolido and Sharon Georgianna, "Durkheim, Suicide, and Religion: Toward a Network Theory of Suicide." *American Sociological Review* 54, no. 1 (1989): 33–48. Adapted from Everton, *Tracking Destabilizing and Disrupting Dark Networks with Social Network Analysis*, 180.

Approaching the same aspect in a similar manner, but using different language, organizational theory posits that networks exhibit flexibility through their balance of differentiation and integration, and the proper balance of these two characteristics provide resiliency. These distinctions by Paul Lawrence and Jay Lorsch determine organizational characteristics in relation to the environmental requirements. Differentiation is the "extent to which actors in a social system are structurally and functionally different from each other."[130] The denser a network, the more integrated it is likely to be, as integration is based on the quality, quantity, and structure of linkages. These linkages may be obtained by formal or informal communication, shared beliefs, common goals, and even organizational structures.[131] The contingency outlook shows that organizations must find the best combination of differentiation and integration for their environment to be most effective.[132] In fighting networks, different skills allow for increased operational complexity. Lawrence and Lorsch found that organizations in more uncertain environments tend to be both more differentiated and place more emphasis on integrating.[133] This would mean that the more dynamic an environment the network is in, the more it is required to decentralize, segment, and increase linkages between nodes. Greater integration at the operational level facilitates fluid actions and inter-operability between nodes in a network. Overall, the ease with which they are able to weigh various aspects of these two qualities and select the appropriate combination determines a network's flexibility.

e. Trust-Based Relations

Networks form primarily through trust-based relationships, which sustain high-risk activity and provide operational advantages. Due to the risk that clandestine activity presents, networks must be decentralized, rely on a unique combination of weak and strong ties, and most importantly, be based on a high degree of trust between

---

[130] Raab and Milward, "Dark Networks as Organizational Problems," 344.

[131] Ibid., 344–345.

[132] Paul R. Lawrence and Jay W. Lorsch, *Organization and Environment, Managing Differentiation and Integration* (Boston: Graduate School of Business Administration, Harvard University, 1967), 238.

[133] Ibid., 157.

members. In fact, trust may even be an essential antecedent condition for the development of network structures, especially ones leading to operational activity. Susan Boon and John Holmes define trust as, "a state involving confident predictions about another's motives with respect to oneself in situations entailing risk."[134] The concise form of this definition highlights the basic elements of trust, and illustrates that trust in not necessarily based on "friendship" or "likes," but rather on predictions in terms of risk. Different levels of trust determine the strength of ties, and illegal, violent networks may have ties ranging from blind trust (rarely), rational calculation, to the strongest form, identify-based.[135]

Primarily, though, the high degree of trust required in fighting networks places an emphasis on identify-based ties within trusted social relationships. According to Raab and Milward, "every secret organization has to solve a fundamental dilemma: how to stay secret and at the same time ensure the necessary coordination and control of its members."[136] Trust provides an element of cohesion and forms ties between actors that create a sense of security, which is crucial to conducting operational acts. The organizational structure of the 9/11 Al-Qaeda attackers "…seems to have been based on prior trusted contacts between members."[137] Bonnie Erickson highlighted this attribute by stating that secrecy is a necessary condition of high-risk activity, and so "…trust becomes a vital matter and hence preexisting networks set the limits of a secret society."[138] The general requirement for trust in networks ensures that linkages are formed from relationships between actors that share a high degree of trust. Clusters of these linkages are also referred to as cliques, which are crucial to ensuring secrecy within an organization. High degrees of trust are primarily evident in the case of strong links, usually based on close ties, such as kinship and friendship. Marc Sageman studied the

---

[134] Susan D. Boon and John G. Holmes, "The Dynamics of Interpersonal Trust: Resolving Uncertainty in the Face of Risk," in *Cooperation and Prosocial Behavior*, ed. Robert Hindle and Jo Groebel (New York: Cambridge University Press, 1991), 167–182, cited in Barbara D. Adams and Robert D. G. Webb, "Trust in Small Military Teams," 1, http://www.dodccrp.org/events/7th_ICCRTS/Tracks/pdf/006.PDF.

[135] Piotr Sztompka, *Trust* (London: Cambridge University Press, 1999).

[136] Raab and Milward, "Dark Networks as Problems," 442.

[137] Ibid., 424.

[138] Erickson, "Secret Societies and Social Structure," 195.

Global Salafi jihadist network in his groundbreaking work, *Understanding Terror Networks*, and found that 68% of all those affiliating with the global jihad had pre-existing friendship bonds. In addition, and a strong indicator of those ties characteristic of tribal organization, kinship played a role in 14% of the mujahedin participating, with entire families involved in some instances.[139] However, it is also important to note that these strong ties may reduce a networks ability to sever ties to increase flexibility, both in overall structure, as well as physical movement.[140]

In addition to enabling participation in high-risk activity, trust also enhances operational activity by increasing the ease of coordination and communication. This performance in high-risk environments is crucial, as, "…the tactical unity of men working together in combat will be in the ratio of their knowledge and sympathetic understanding of each other."[141] High levels of trust allow for intent, rather than directive mission orders, and ensure a common outlook. Robert Coram states, "trust emphasizes implicit over explicit communications. Trust is the unifying concept. This gives the subordinate great freedom of action."[142]

One of the primary means of forming trust is a shared ideology, or cause, and it provides an over-arching umbrella for other relationships, motivations, and geographic origins in networks. Throughout history, guerrillas and those involved in armed opposition have been united under a common cause, motivated by grievances, and inspired by common beliefs and values. These ideological motivations provide a common umbrella from which to organize. In discussing the al-Qaeda organization, Ronfeldt states that it is held together "…by a gripping sense of shared belonging, principles of fusion against an outside enemy, and jihadist narrative so compelling that it amounts to both an ideology and a doctrine."[143] This use of ideology as an organizing element is also a function of tribal structures, where religion and kinship are fused to provide a nearly

---

[139] Sageman, *Understanding Terror Networks*, 112.

[140] Eilstrup-Sangiovanni and Jones, "Assessing the Dangers of Illicit Networks," 26.

[141] Marshall, *Men Against Fire*, 61.

[142] Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (New York: Back Bay Books, 2004), 337.

[143] Ronfeldt, "Al-Qaeda and its Affiliates," 43.

comprehensive sense of identity. Weak ties that share a common ideological milieu might provide a more significant bond than would otherwise be the case. Those outside this identity are viewed as "others" and are not trusted, where those who share a common identity are granted a great deal of trust.

f. Decontrol

Networks rarely exhibit direct command and control, which provides flexibility and autonomy in tactical decision making, but may decrease collective direction and efficiency. Leadership in a network provides overall strategic direction and purpose, but seldom more than necessary to synchronize action. This leadership direction is instrumental in mobilizing and organizing, as well as providing an overall element of cohesion, but it rarely takes direct control of nodes. The authority that exists in networks is not focused on direct control, and differs from standard military authority that emphasizes hierarchical command. Instead, it provides direction and inspiration with lines of authority less rigid than in a hierarchical organization, striving for "decontrol."[144] However, negative aspects of a lack of centralized leadership exist. Decision making may be complicated and protracted when trying to achieve organizational consensus and direction.[145] While complex decisions at the small unit level may occur rapidly due to increased autonomy, decision making for the entire network may occur less efficiently. Rapid decisions made by autonomous nodes or individual actors are seldom synchronized without unity of purpose and communication.

The noted sociologist, Georg Simmel held that secret organizations were deliberately built by a central power and required a great degree of authority to maintain control.[146] However, this hierarchical view of clandestine organizations fails to account for the dynamics of risk in irregular warfare, and the fact that pre-existing networks tend

---

[144] John Arquilla, *Aspects of Netwar & the Conflict with Al-Qaeda* (Monterey, CA: Naval Postgraduate School, Information Operations Center, 2009), 4.

[145] Walter W. Powell, "Neither Market nor Hierarchy: Network Forms of Organization," *Research in Organizational Behavior* 12 (1990): 318.

[146] George Simmel, "The Secret and the Secret Society," ed. and trans. Kurt Wolff, *The Sociology of Georg Simmel* (New York: Free Press, 1950), 357.

to form the basic structure of most secret organizations.[147] Still, the requirement for security in a clandestine organization requires some amount of authority to ensure compartmentalization—where relationships and linkages are kept to a minimum. This requirement would likely produce a hierarchical method of control, except for the organizational requirements to remain decentralized. Leadership in networks requires an element of vertical authority, where a leadership figure might provide direct guidance, but also a high degree of decentralized authority, relying on individual nodes to maintain security. By providing less directive control, leadership in networks ensures that each element has the maximum amount of autonomy. Leadership plays a less active role in controlling decentralized and autonomous fighting elements. According to Hoffman, this is an increasing characteristic of terror networks where "this phenomenon, variously termed 'leaderless resistance,' 'phantom cell networks,' 'autonomous leadership units,' 'autonomous cells,' 'networks of networks,' or 'lone wolves,'…has become one of the most important trends in terrorism today."[148] These networks display collective security not through a centralized authority, as in traditional guerrilla or terrorist organizations, but rather through cultural norms and the necessity to ensure operational security to survive.

3. Doctrine

Military doctrine seeks to determine the way in which warfare occurs, and characterizes the fundamentals that guide the application of military forces. Doctrine influences all levels of warfare and provides "fundamental principles" that guide operational practice to achieve strategic goals.[149] According to General George H. Decker, "doctrine provides a military organization with a common philosophy, a common language, a common purpose, and a unity of effort."[150] Historically, doctrine is

---

[147] Erickson, "Secret Societies and Social Structure," 195.

[148] Hoffman, *Inside Terrorism*, 271.

[149] U.S. Department of Defense, Joint Publication 1-02, *Dictionary of Military and Associated Terms*, 524.

[150] U.S. Department of Defense, Joint Publication 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: U.S. Government Printing Office, I–1.

used as a term that defines critical components of a national security policy, and is guided by grand strategy. Doctrine describes how military forces organize, and how they will counter threats to national security, and it usually takes the form of offensive, defensive, or deterrent action.[151] Offensive doctrine seeks to disarm an adversary, usually through destroying their armed forces. A modern example of offensive military doctrine is the U.S. Army's Air Land Battle doctrine developed in the 1980s, which emphasized deep-strikes behind "front-lines" using long-range fires, while maneuver forces exploited weaknesses to attack follow-on forces.[152] Defensive doctrine emphasizes denying an adversary the objective that they seek. The aim of deterrent doctrine is to punish an aggressor by raising their costs.[153]

An opponent's military doctrine reveals the expectations of its leadership, its preferred manner of waging war, its capabilities, the resources it acquires, and its type of forces. Doctrine enables strategy by providing the means and ways to conduct warfare, enabling strategy's employment of "…power in a synchronized and integrated fashion…."[154] Networks seek to use all manner of resources in their employment of strategy, and there are no purely military means, which restrict their development of doctrine. In addition, the fundamental nature of irregular warfare is a competition involving the population, not just military means, and so the scope of doctrine available to a network is arguably wider than that available to a professional force focused intently on military affairs. While professional militaries traditionally employ doctrine that consists of offensive, defensive, or deterrent forms, networks are not limited by these strict constructs and blur characteristics over time and through the space of an irregular conflict.

---

[151] Barry Posen, *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars* (Ithaca, New York: Cornell University Press, 1984), 13.

[152] Robert H. Scales, *Certain Victory: The U.S. Army in the Gulf War* (Washington, DC: Brassey's, 1994), 26.

[153] Posen, *The Sources of Military Doctrine*, 14.

[154] U.S. Department of Defense, Joint Publication 1-02, *Dictionary of Military and Associated Terms*, 524.

Networks also have doctrine, but it is much less formalized, or structured than professional militaries. By incorporating certain elements of unconventional warfare and updating with modern "best practices," networks display the ability to rapidly evolve doctrine in ways that traditional militaries find challenging. As a strategist for the al-Qaeda network (and perhaps one of the most noteworthy strategists since Mao), Abu Musab al-Suri references "Mao Tse-Tung, Guevara, Giap, Castro, and others," calling them the "greatest theoreticians in military art," as he cautioned against a tactical defense for the Al-Qaeda network.[155] Al-Suri provides a clear example of the use of guerrilla warfare as an element of this network's doctrine, stating, "…one has to establish firmly the principles of the Islamic doctrine in general, and the jihadi doctrine in particular." Expanding on this topic, "it is also necessary to focus on understanding the theory of guerrilla warfare in general, and the basis for jihadi guerrilla warfare in particular."[156] Yet, it is far too simplistic to describe al-Qaeda as a guerrilla organization as they have transcended traditional practices by their skilled utilization of the network form and netwar principles. Quite simply, just as it does for a professional military, doctrine provides principles for networks in conflict.

In their insightful article, "The Strategies of Terrorism," Andrew Kydd and Barbara Walter show that terrorists employ a doctrine based on costly signals. This doctrine of signaling highlights the unique combinations of offensive, defensive, and deterrent doctrine that networks employ.[157] Terrorist violence, or the act of terrorism, is designed to achieve an intended result, and in many instances, it seeks to both convey a message and provoke a reaction. "Terrorism works not simply because it instills fear in target populations, but because it causes governments and individuals to respond in ways that aid the terrorists' cause."[158] The five principle "strategies" that Kydd and Walter identify as a part of their signaling doctrine are: 1) attrition, 2) intimidation, 3)

---

[155] Brynjar Lia, *Architect of Global Jihad: The Life of Al-Qaeda Strategist Abu Mus'ab al-Suri* (Cambridge University Press India, 2008), 373.

[156] Lia, *Architect of Global Jihad*, 475.

[157] Andrew H. Kydd and Barbara F. Walter, "Strategies of Terrorism," *International Security* 31, no. 1 (2006): 58.

[158] Ibid., 50.

provocation, 4) spoiling, and 5) outbidding.[159] Each of these forms of terrorist strategy involves offensive attacks, and it would appear that terrorism has an offensive doctrine. However, terrorist organizations, like most networks, are inherently weaker than their nation-state opponents, and terror tactics provide a means to achieve defensive aims by also denying an adversary the objective they seek. In addition, the doctrine of signaling also has a deterrent component, as it aims to punish an aggressor and so raise their costs without reducing the terrorists' own.[160]

While much of doctrine is focused on traditional warfare, with an emphasis on the principles of war that favor nation-states, irregular warfare contains other principles and strategies. While networks lack the formalized, and perhaps limiting, doctrine of modern nation-states, they draw on timeless principles of irregular warfare. These principles have shaped irregular action for as long as the weak have confronted the strong, and they place special emphasis on elements, such as surprise and deception. Most notably, networks utilize doctrinal principles that are fluid in nature, and that foremost, seek to ensure that the network is able to adapt to changing circumstances. Rather than seek to entrench doctrine, in the bureaucratic nature of hierarchical militaries, networks view doctrine as a free-flow exchange of innovative ideas. The doctrinal characteristics described in this section emphasize this ability to flex, and to wage war in a manner consistent with the situation at hand, rather than attempt to fight based on fixed means. For these reasons, networks blur the lines between strictly offensive or defensive doctrine, and utilize elements of population-centric strategy foreign to conventional military forces. Network-style warfare provides distinctive doctrinal attributes, which provide dramatic change from even fairly recent notions of unconventional warfare.

a. Blurring of Offense and Defense

Networks fight using a unique combination of doctrine, which often blurs offensive and defensive attributes. While conventional conflict traditionally occurs between two militaries occurs vis-à-vis their forces, the conflicts in irregular warfare

[159] Kydd and Walter, "Strategies of Terrorism," 51.

[160] Posen, *The Sources of Military Doctrine*, 14.

more directly involve the population. This conflict makes it difficult to define doctrine in such straightforward terms as offense and defense, which traditionally describe relationships between military forces. However, attributes of offense, defense, and deterrence are incorporated in netwar doctrine, which often present themselves in blended forms.

In many cases, networks will seek to frame their struggle through defensive terms at the strategic level, while at the same time, conducting offensive attacks. Existing force asymmetries mean that networks mainly use the offensive when they have the initiative. "It is the secret of the guerrilla force that, to be successful, they must hold the initiative, attack selected targets at a time of their choosing, and avoid battle when the odds are against them. If they maintain their offensive in this way, both their strength and their morale automatically increase until victory is won."[161] Despite his focus on conventional war between nation-states, even Clausewitz's strategic thinking recognized that irregular actions provided a potent defensive tool.[162] Often, the strategic goal of networks is not to defeat opposing forces in a decisive manner, but show a stronger will, and thereby, defeat their will to continue fighting. The aim of defeating the will of an opponent focuses on both the will of the military adversary, as well as the will of the people who support it. Popular will may prove decisive within irregular warfare, and by maintaining the strategic defensive, networks can preserve their forces, prolong the conflict, and thereby, wear down their opposition. "They will play the part of a vicious gnat stinging and eluding a larger, rather clumsy beast, until it retreats in fury and frustration."[163] Networks defend in aggressive fashion, seeking to inflict damaging blows through a combination of ambushes and swarming attacks. These offensive actions are utilized to deny the enemy its objective, and are incorporated in a defensive strategy whose pro-active nature is remarkable. While it will be explored further in a case study, the Chechen response to the Russian invasion in 1996 provided hallmark examples of

[161] Sir Robert Thompson, *Defeating Communist Insurgency: The Lessons of Malaya and Vietnam* (New York: Praeger Publishers, 1966), 115.

[162] Carl Von Clausewitz, *On War*, Michael Howard and Peter Paret, ed. and trans. (Princeton, NJ: Princeton University Press, 1989), 482.

[163] Paget, *Counter-Insurgency Operations*, 27.

offensive actions that sought to inflict serious damage on advancing Russian forces, culminating in the initial battle for Grozny.[164] The Chechen response even took the conflict beyond its borders to include strikes inside Russia and demonstrated information operations synchronized with action.

Tactically, networks tend to remain on the offensive and avoid fixed defensive engagements. Strategists throughout history have identified that irregular forces must be tactically offensive, and that they will be quickly overwhelmed if attempting to fight defensively at the tactical level. Modern-day networks are no different, and their operations are offensively focused. Despite a general force disadvantage, networks fight offensively, and mitigate their lack of superior mass and firepower through surprise, rapid or indirect attacks, and the ability to engage and re-engage in a way that maintains relative power. At the tactical level, networks utilize tactics, such as swarming to great effect, as clearly demonstrated by the swarms of vehicle-born improvised explosive device (IEDs) that terrorized Baghdad during al-Qaeda in Iraq's (AQI) struggle for control of that city. Traditionally irregular forces would incur tremendous risk by attempting tactical defensive action, but a blurring of offensive techniques, such as the ambush, or swarming, enables networks with defensive aims. These forms of aggressive action are typically considered in offensive terms, but may occur to achieve a defensive objective, or in response to an opponent's attack, demonstrating the fluidity of network doctrine.

b. Swarming

Networks utilize swarming as a fundamental aspect of their doctrine, and one that provides a distinguishing element from other forms of irregular war. Swarming describes the combined offensive action of small, highly mobile forces that attack and withdraw in a pulsing manner.[165] The requirements for effective swarming attacks are large numbers of smaller units that have the ability to coordinate with each other

[164] John Arquilla and Theodore Karasik, "Chechnya: A Glimpse of Future Conflict?" *Studies in Conflict and Terrorism* 22, no. 3 (July–September 1999): 208.

[165] Arquilla and Ronfeldt, *Swarming and the Future of Conflict*, 8.

autonomously, as well as a command element just as connected, but that exerts control only when required.[166] Swarming is a unique doctrine that allows numerous small elements the ability to attack swiftly in mass, but still possess the ability to disperse rapidly when necessary. Swarming is not limited to physical forces, but most notably includes long-range fires and the employment of sensors in ways that simultaneously enable synchronized action. As Sean Edwards describes, "swarming occurs when several units conduct a convergent attack on a target from multiple axes. Attacks can either be long range fires or close range fire and hit-and-run attacks."[167] Swarming provides a method of warfare uniquely suited to the high information levels, but overall decentralized structure that characterizes fighting networks.

Swarming occurs throughout history, and irregular forces, such as the Finnish army in their remarkable campaign against the Russian invasion in 1939–1940, utilize aspects of swarming with great effect.[168] While employed by guerrillas at times, swarming doctrine highlights key differences separating networks in conflict from guerrilla warfare. First, guerrilla warfare is generally employed by an inferior force, and in support of insurgent, or political goals. As Liddell Hart emphasized, "in the past, guerrilla war has been a weapon of the weaker side, and thus primarily defensive…."[169] Further, and most importantly, guerrilla warfare primarily employs hit-and-run tactics by small units, which achieve little decisive effect against an enemy because they are limited in scope and lack synchronized action. Swarming emphasizes multiple nodes that attack in a synchronized manner and are capable of conducting the repeated and decisive action, which displays the power of a networked force. This ability to conduct sustained pulsing attacks by multiple units clearly differentiates swarming from standard guerrilla warfare.[170] While swarming presents a tremendous advantage to weaker forces, if they are sufficiently networked, forces of any type may also employ it.

---

[166] Arquilla and Ronfeldt, *Swarming and the Future of Conflict*, 22.

[167] Edwards, *Swarming and the Future of Warfare*, xvii.

[168] Eloise Engel and Lauri Paananen, *The Winter War: The Soviet Attack on Finland 1939–1940* (Mechanicsburg, PA: Stackpole Books, 1973).

[169] B. H. Liddell Hart, *Strategy* (New York: Frederick A. Praeger Publishers, 1954), 367.

[170] Edwards, *Swarming and the Future of Warfare*, 69.

While swarming is not unique to irregular warfare, fighting networks utilize swarming due to their decentralization and a high degree of information. The following figure depicts the relationship between these components and shows a trend line depicting the overall nature of warfare to-date. Fighting networks generally fall within the center of the upper-left quadrant. Swarming has three important enablers on which it relies: elusiveness, superior situational awareness, and standoff capability.[171] Elusiveness is generally a function of stealth and a network's ability to remain concealed, while situational awareness results from information shared in a networked fashion. Standoff capability reflects the employment of fires and indirect weapons, while at the same time, keeping nodes from being directly targeted (through either greater range and/or concealment). A recent emphasis on swarming doctrine is the mysterious Abu Bakr Naji's publication in *Sawt al-Jihad*, the al-Qaida Internet magazine, urging jihadists to "strike with your striking force multiple times and with the maximum power you possess in the most locations."[172]

[171] Edwards, *Swarming and the Future of Warfare*, 117.

[172] Abu Bakr Naji, "The Management of Savagery," in *The Canons of Jihad*, ed. Jim Lacey (Annapolis, MD: Naval Institute Press, 2008), 62.

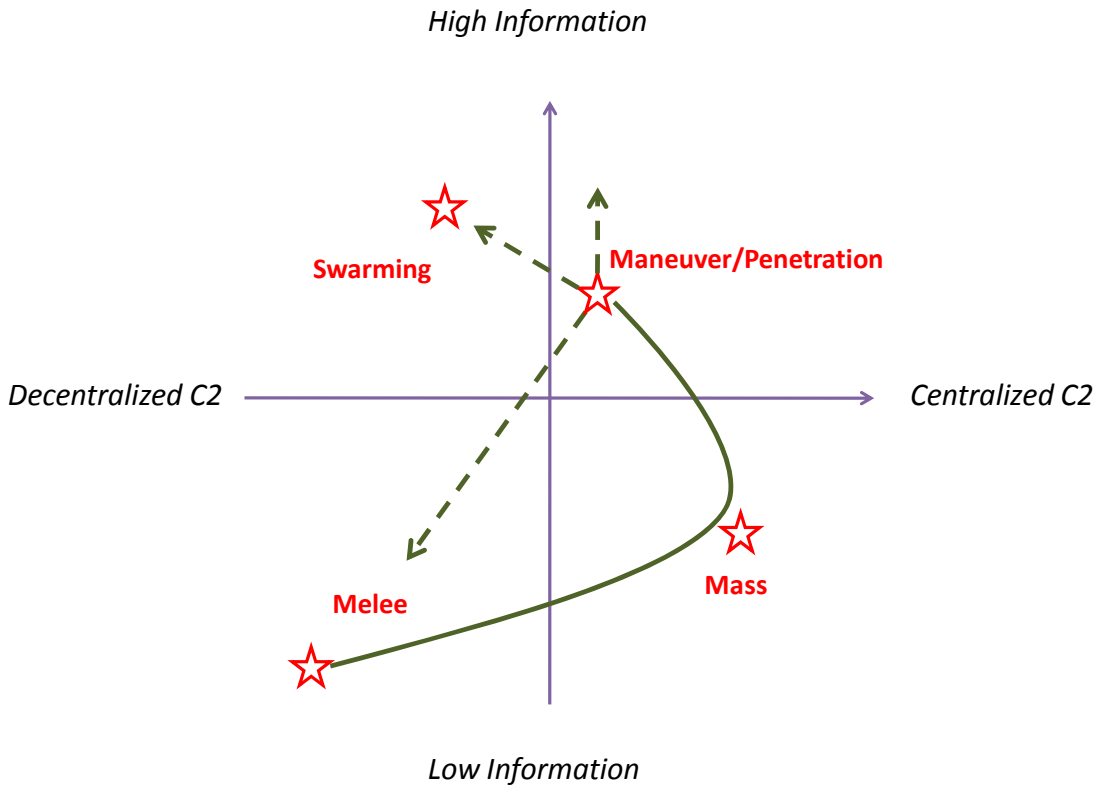

Figure 8. Four Forms of Warfare with General Trend-Line Depicting Overall Employment[173]

c. Protracted and Rapid Warfare

Networks are capable of fighting in a protracted manner, but will take the initiative when it presents itself, which demonstrates staying power, but also seizing on opportunities for rapid victory. While the asymmetry of irregular conflict generally promotes being able to "outlast" instead of directly "outfighting" superior opponents, this does not exclude decisive action. Networks differ from classic irregular opponents, which primarily use guerrilla warfare strategies based on minor actions. The most common guerrilla strategy is a classic war of exhaustion, one that seeks to wear down the opponent

[173] This diagram was created by Michael Freeman, and based on the relationship between command and control (C2) and information levels described in Arquilla and Ronfeldt, *Swarming and the Future of Conflict*, 7.

using smaller attacks that gradually weaken their opponent's military forces. Another classic strategy is based on continuing to disrupt the enemy while attempting to build forces from an irregular army to a larger regular army able to confront a superior opponent conventionally. The end state of this focus is Mao's third phase of guerrilla strategy, which he describes as a "war of movement," and which culminates in conventional warfare capabilities. Networks rarely use these two strategies, but as complex adaptive systems, networks are able to generate remarkable powers of survivability and persistence.[174]

Another strategy, which is perhaps most applicable to modern networks, is simply persisting in attacks against any element of power (to include military forces, civilian will, and economic centers). This form of attack may require considerable time because it requires a combined approach that is actually a total war, but conducted in an irregular manner. As well, systems disruption's primary approach is swarming, which if conducted in a pulsing manner, may require additional time to wear down an opponent.[175] Since its focus is on total war, and unlimited attacks on any aspect of its opponent's power, this approach will generate considerable pressure against the network. This pressure requires a flexible approach, and operational activity able to oscillate between periods of intense activity and dormancy, to prevent compromise and ensure persistence over time. This strategy most closely describes the nature of al-Qaeda's campaign against Western interests.

Another situation that clearly illuminates fighting networks is the combination of persistence and decisive victory displayed by the Chechen devolution from a semi-professional military force, into smaller bands of highly trained fighters. Instead of following a classic guerrilla strategy of building into a conventional force, these bands utilized their professional training in organizational and doctrinal ways that favored their decentralized clan-based relationships. Most militaries would have crumbled out of their hierarchical structure; a disintegration, which the Russians expected. However, the Chechens were able to metastasize into a formidable network,

[174] Duffield, "War As a Network Enterprise: The New Security Terrain and its Implications," 158.

[175] Edwards, *Swarming and the Future of Warfare*, 105.

and thereby, persist against the Russian offensive.[176] Network opponents are able to persist over time, and utilize the context of their situation to fashion campaigns, which favor their ability to resist in multiple ways. They balance the need for operational activity with the need for persistence, which is complimented by structural aspects of resiliency on an operational level.

d. Deception

Networks rely heavily on deception, largely in the form of concealment, to ensure favorable conditions from the tactical through strategic levels. Deception is paramount in warfare of all types, but Sun Tzu's aphorism holds greater value in irregular warfare, "All warfare is based on deception. Therefore, when capable, feign incapacity; when active, inactivity. When near, make it appear that you are far away; when far away, that you are near. Offer the enemy a bait to lure him; feign disorder and strike him."[177] Networks employing deception in irregular warfare gain significant advantages through various stratagems, which seek to gain a relative force advantage.

Tactically, networks rely on elements of deception to infiltrate an area of operation and it plays a primary role in achieving surprise against stronger opponents. Fighting networks rarely utilize uniforms, and generally lack distinctive markings. Their appearance as a member of the civilian population provides a tremendous amount of concealment, so much so that in professional militaries, only selected organizations are granted this ability, and even then, it has traditionally carried a distasteful notion of subterfuge. These distinctions are irrelevant to networks and they utilize every advantage possible to conceal their intentions and deceive the nature and manner of their attacks. For this reason, terrorism is a powerful tool employed by networks, as it carries the shock of surprise, and a devastation that is both concealed and unexpected.

At the strategic level, networks maintain their defenses through their ability to hide, in real or virtual domains, or conceal themselves. The asymmetry in force

---

[176] Shcultz and Dew, *Insurgents, Terrorists, and Militias*, 139.

[177] Tzu, *The Art of War*, 66.

requires those waging irregular war to remain undetected. The advantage of being able to hide within the population or difficult terrain provides advantages to a networked force. The primary means of concealment for networks is to blend into the general population, and utilize day-to-day activity as a means of concealing oneself and disguising operational activity. In many cases, this is as simple as only taking up arms, or conducting identifying activities, when conducting operations. Within a larger population base, enough anonymity exists to achieve greater operational freedom, especially if the existing relationships might constraint activity.

e. Systems Disruption

Networks attack weakness using systems disruption, in addition to directly confronting an opponent's forces. The concept of systems disruption is a form of indirect strategy, and perhaps represents the apex of indirect attacks. As the noted strategist B. H. Liddell Hart stated, "the true aim is not so much to seek battle as to seek a strategic situation so advantageous that if it does not of itself produce the decision, its continuation by a battle is sure to achieve this."[178] T. E. Lawrence, in his irregular campaign during WWI, focused on destroying the Turkish army's scarce material resources, rather than confronting their larger forces, and in doing so, he formulated a new theory of irregular warfare, one that focus more on a winning strategy, than on winning battles.[179]

The idea of system disruption employed by networks uses the same principles, but focuses on all aspects of an opponent's power, not simply military forces. The strategic nature of these attacks reveals themselves in terror strikes, which also "seek to impose severe and growing economic costs on their targets."[180] Today's nation states exist on arteries of fuel, electronic grids, power generation, transportation, and inter-connected computer systems. These systems provide new targets for networks, which target them as a way to weaken their opponent's resource base, economy, and

[178] Hart, *Strategy*, 365.

[179] B. H. Liddell Hart, *Lawrence of Arabia* (New York: DeCapo Press, 1989), 138.

[180] John Arquilla, "The End of War as We Knew It? Insurgency, Counterinsurgency and Lessons from the Forgotten History of Early Terror Networks," *Third World Quarterly* 28, no. 2 (2007): 377.

transportation capability.[181] Iraqi insurgents targeted coalition force convoys with IEDs, to damage and disrupt the flow of material resources, more than inflict casualties, but more tellingly launched hundreds of attacks against population centers and industrial targets. On the global level, al-Qaeda strategy promotes attacks on economic systems, as seen in attacks against petroleum related infrastructure in Saudi Arabia and the Gulf States. Abdul Aziz al-Muqrin, the operational commander of al-Qaeda in the Arabian Peninsula (AQAP) paraphrased similar writing from Ayman al-Zawahiri and Musab al-Suri when he stated that the "purpose of these targets is to destabilize the situation and not allow the economic recovery….to have foreign investments withdrawn from the local markets."[182] Systems disruption provides a form of doctrine that enables fighting networks to fight nation states on a strategic level, through the "sabotage of critical systems to inflict economic costs on the target state."[183]

4. Operational Methods

Operational methods focus on the operational and tactical level of warfare, while recognizing that the traditional levels of war are not clear distinctions in irregular warfare. Since networks fight with smaller numbers, yet seek to have a disproportionate effect on popular perception, there is significant crossover, with tactical actions producing tremendous strategic effect, and strategy hinging on tactical behavior. For this reason, operational methods describe the blend of activities that occur at the operational and tactical levels, and reflect the integration of information strategy. Operational methods stem from doctrine; hence, aspects like flexibility, surprise, concealment, and adaptability are fundamentals of irregular tactics. These fundamentals allow for improvisation at the operational level, where networks seek to achieve significant strategic effects through each tactical action. The operational level of war blends tactics and strategy, synchronizing the means of tactical actions with the goals of strategic

---

[181] Robb, *Brave New War*, 95.

[182] IntelCenter, *Al-Qaeda Targeting Guidance*, vol. 1.0, Thursday, April 1, 2004 (Alexandria, VA: Tempest Publishing, 2004), 6–9; originally from Abd al-Aziz al-Muqrin, *Al-Qa'ida's Doctrine for Insurgency: "A Practical Course for Guerrilla War" Translated and Analyzed by Norman Cigar*, trans. Norman L. Cigar (Dulles, VA: Potomac Books, 2009).

[183] Robb, *Brave New War*, 95.

objectives. According to U.S. military joint doctrine, actions at the operational level are a form of art, which requires imagination, skill, knowledge, and experience to organize and employ military forces in campaigns.[184] The operational level of war is the crucial aspect of warfare, and networks understand this, as well as professional armies. Al-Suri describes operational theories and an organizational setup based on a "system of action: not a secret organization for action," and discusses how the "Islamic Resistance units develop their operational methods…with regards to the military theory…."[185]

Tactics are focused on combat actions, and seek to describe the art and science of actions that occur on the battlefield. This includes the technical application of techniques and procedures, and modern military doctrine usually combines all three of these aspects into a comprehensive whole of tactics, techniques, and procedures (TTPs). Network tactics also include "engagements," and "activities," recognizing that the battlefield may not be the primary space for irregular conflict.[186] Networks succeed at the tactical level far more than at any other level, primarily because their operational methods favor small, decentralized units of action rather than larger ones requiring much operational synchronization.

Information technology provides the means to achieve greater internal and external communications and it has tremendous effects on operational methods. The tools and resources that information technology provides contribute to the operational methods employed by networks, and perhaps more than any other factor, have added increased viability to these methods. The primary aspect of enhancement is internal communications. Networks utilize modern information technology to increase the amount of communications that occur between otherwise disconnected, decentralized elements. While radios have provided some of this connectivity in irregular warfare, the rapid proliferation of cellular phones allows every single node in the network the ability to communicate with another. This degree of communications, which surpasses that of most

[184] U.S. Department of Defense, Joint Publication 3-0, *Joint Operations* (Washington, DC: U.S. Government Printing Office, 2010), II–2.

[185] al-Suri, "The Global Islamic Resistance Call," in *Architect of Global Jihad*, 440.

[186] U.S. Department of Defense, Joint Publication 3-0, *Joint Operations*, xiii.

modern armies, enhances their ability to decentralize, increases mobility, and allows for synchronizing activities. Moreover, this increased use of technology provides networks with the ability to acquire greater standoff, leading to an increase in number and lethality of indirect attacks. This standoff is a critical part of a swarming doctrine, and information technology provides the means to coordinate such action further, as well as the physical technology to launch attacks. A disposable cell phone provides the means both to coordinate explosive swarming attacks and serves as the tool to initiate the actual detonations.

Operational methods function as a blend of operational art and tactical application that utilizes information technology in a system remarkably adaptable to the revolutionary aspects of the information age. While there are doctrinal characteristics, which provide some guidelines for the application of force, the fundamental nature of network operational methods lies in the willingness to combine multiple aspects of the irregular warfare environment in a system that is both coherent, yet shifting. The following characteristics seek to provide additional clarity to the complex ways in which networks actually engage in violent activities.

a. Economy of Force

Networks generally lack resources compared to their opponents, but being lightly armed provides multiple operational advantages. A lack of resources actually provides some advantages to the irregular opponent, and illustrates the principle of economy of force. Economy of force is a fundamental principle of war, and describes the "judicious employment and distribution of forces," which is critical given networks' small elements and lack of redundant capabilities.[187] While much of modern warfare hinges on resource production, fewer resources mean that networks have little to defend, less to transport, and require less sustainment for operational activity. Limited resources provide an antecedent condition that contributes to network doctrine, shapes tactical application, and shapes much of their capacity for action. In some cases, the idea that less is more actually rings true and networks are unencumbered by excessive equipment and

[187] U.S. Department of Defense, Joint Publication 3-0, *Joint Operations*, A–2.

the logistical requirements they entail. Much like an alpinist that moves through vertical terrain with greater speed, achieving less risk than climbers that attempt to siege with heavy equipment over greater time, networked fighters move faster because they are lighter. Tactically, the use of economy of force provides a significant maneuver advantage to the small elements within networks.

The corollary to limited resources is that a constant requirement exists to gain sufficient resources. Networks accomplish this gain primarily by taking, or utilizing the resources of their logistically superior opponent. Raids and ambushes are launched with the purpose of harassing the enemy, but also to gain resources. In this manner, logistical requirements are fairly simple—networks utilize their opponent's assets. This ideal has perhaps found its furthest expression in al-Qaeda's use of aircraft as weapons for the September 2001 attacks. Armed with next to nothing, these irregular warriors succeeded in launching a devastating attack using their opponent's resources and tools. In fact, it was their lack of resources, or a tremendous display of economy of force, that allowed them to infiltrate their target area and achieve surprise. If the 9/11 hijackers had attempted to use even the lightest military armament to accomplish their operation, the likelihood of their detection and subsequent failure would have been much higher. This ability to infiltrate as a member of the population, with no weapons, provides a tremendous advantage to networks.

In many situations, resources and technology may be increasingly available and inexpensive, to the point where networks rarely concern themselves with logistical matters, but instead utilize the tools and technologies readily available in everyday use. Information technology is a critical tool that allows tremendous economy of force, and their ability to extend their base of support in a global dimension. Frank Hoffman, in describing modern terrorist networks notes that "modern irregular warriors," are not limited to the weapons they've always had, but now "…include the mini-cam and videotape, editing suite and attendant production facilities; professionally produced and mass-marketed CD-ROMs and DVDs; and most critically, the laptop and desktop computers, CD burners and e-mail accounts, and Internet and World Wide Web

access."[188] The number of laptop computers recovered by those combating these networks in remote desert locations and mountainous terrain reinforces the ubiquitous nature of this modern force multiplier.

b. Stealth

Networks display a high degree of stealth, which is a fundamental attribute of their tactical decision making. Stealth provides networks with the capability to conduct surprise attacks, use the ambush as a defensive maneuver, and ensure a secure disengagement or evasion when necessary. Stealth is best described as a combination of mobility and concealment, or the ability to move undetected. Stealth highlights the use of concealment and deception and is another example of the way networks blend various attributes. Networks must maintain a high degree of mobility to ensure survivability, an attribute which reinforces their concealment capability. Mobility allows a small element to move and avoid being found, and most importantly, if found, rapidly withdraw to avoid a tactical defense and the risk of destruction. Since an irregular force's numerical strength is generally inferior, and because it is primarily focused on survival, the primary aspect of its tactics is evasion.[189] The ability to evade generally connotes a defensive aspect, but it also allows irregular opponents to conduct offensive attacks against superior opponents. The small size of independent nodes dictates that they conduct attacks where unexpected, which requires being able to move rapidly, and then to ensure a fast withdraw to initiate other attacks. In fact, this forms an offensive cycle, where an irregular opponent's mobility determines the tempo of offensive operations possible to conduct. In addition, mobility by itself is of some value, but provides little advantage if networks are not able to conceal themselves as well.

The requirement for maintaining stealth presents a challenge depending on the degree to which irregular opponents require a connection with the population. One of the ways they maintain this connection is through an increased use of information

---

[188] Frank G. Hoffman, "Mind Maneuvers," *Armed Forces Journal*, April 2007, 1, http://www.armedforcesjournal.com/2007/04/2550166/.

[189] Robert Taber, *War of the Flea: The Classic Study of Guerrilla Warfare* (Washington, DC: Potomac Books, 2002), 154.

technology, which provides a distributed means of connecting with the larger population. Physical access is not necessarily the requirement as it was for traditional guerrilla warfare. Information technology plays a significant role in allowing networks to balance mobility with connection. The media, and especially the use of the Internet, provides a means to ensure that a network's messaging is connected to the population despite having to remain mobile and concealed.

c. Surprise

Networks require surprise, which provides the decisive element in attacks against stronger opponents. Whether these offensive actions take the form of direct attacks or indirect attacks, they rely on the fundamental element of surprise. At its basic level, surprise allows for weaker opponents to achieve considerable effects with minimal force. As Richard Simpkin states in his chapter on small-force maneuver theory, "given free reign, surprise is a matchless combat multiplier. Revolutionary warfare exploits it to carry the principles of economy of force to lengths unimaginable to the conventional military mind."[190] Surprise is a principle of war, and is sought by all military forces, but lightly armed irregular forces require it to maintain operational effectiveness. Networks utilize surprise gained from their emphasis on stealthy movement and an overall focus on concealed action. Surprise is a key tactical attribute, but is also displayed operationally, as seen in network-style offensives, such as those displayed by Chechen fighters in 1996.

Tactically, the primary forms of direct attacks are raids and ambushes, whose basic principles are incorporated into aspects of swarming. Both forms require the same principles of precise intelligence and solid planning to achieve surprise. In both of these methods of attack, irregular opponents are directly confronting their enemy, and seeking to maximize their strengths against the enemy's weaknesses. Further, surprise overcomes a potential offset in numbers and firepower, which creates a window of advantage. Detailed planning, with an emphasis on terrain, coordination, and intelligence, allows networks to confront their opponents with the highest degree of success. For this

[190] Richard E. Simpkin, *Race to the Swift: Thoughts on Twenty-First Century Warfare* (London: Brassey's, Inc., 2000), 320.

reason, networks rarely conduct movement to contacts, or hasty attacks, because the chance of achieving surprise are relatively low, and the nature of the engagement cannot be controlled. In contrast, a raid achieves surprise through good intelligence, and is distinguished by other forms of attack by a swift infiltration and a planned withdrawal. More than any other form of offensive attack, the raid relies on a high degree of stealth. An ambush achieves surprise by concealment and maximizes its effects through a careful selection of the terrain.[191] Networks also conduct strikes by assassination, which is a form of attack that directly targets individuals. Assassinations are particularly effective because of their precision, and are generally used to eliminate specific individuals within the opposition, to deny critical skills, or for general terror effects.

Indirect attacks have two main forms, the use of indirect fire weapons, such as mortars, rockets, and improvised launched explosives, and the use of remotely detonated IEDs. Both aspects maximize the attribute of surprise, while providing the added benefit of less risk to force. Swarming employs indirect attacks alongside direct engagements to maintain the element of stand off where forces are unable or unwilling to directly clash.

Networks employ surprise at the tactical level, but also in their innovation in doctrinal ways. The ability to adapt is crucial to achieving surprise, and the evolution of IEDs shows how a form of attack is continually adapted to overcome countermeasures. The evolution from using radios to detonate IEDs to the use of common items, such as garage door openers, remote car-door openers, and cellular phone technology, provides a tremendous advantage in achieving surprise because these items are commonly used. The next evolution in network indirect attacks is very likely to come in the form of weapons of mass destruction (WMD), with devastating effects.

[191] The ambush is a form of offensive attack that utilizes principles of the defense and relies on deception. Jon Latimer describes the ambush and "…the use of lures to draw the enemy into them…" as fundamental aspects of irregular and guerrilla warfare; Jon Latimer, *Deception in War* (New York: Overlook Press, 2001), 269.

d. Clandestine Mechanisms

Networks require clandestine mechanisms to maintain secrecy, but they create operational inefficiencies. Communications are a critical part of maintaining an organization of any type, especially a robust network requiring synergistic effects of small, often diverse activities in a complex irregular war. Networks require some degree of communications to establish themselves, organize, and pursue a common vision and purpose. All of these requirements are difficult for organizations in general, let alone a decentralized organizational structure operating at great risk. The requirements for secrecy impose a tremendous cost on network's ability to communicate both internally, and to a degree externally. In fact, the very existence of communications provides a linkage that if discovered, reveals organizational attributes. For this reason, networks rely on clandestine mechanisms, which shape the organizational structure, and type of communications. However, the pressures to remain as clandestine as possible conflict with the ability to maintain strong social ties, influence the greater population, as well as achieve operational efficiency. An idealized clandestine structure, with compartmentalization, works well in theory, but requires tremendous control, time to establish, and is generally operationally inefficient.

Organizations must communicate to exist, and in many situations, a compromise occurs between the restrictions of secrecy and the requirements for speed and flexibility. "Even in optimum circumstances communication problems tend to have the most severe effects both on the pursuit of the armed struggle and on the internal nature of the rebel organization. Secrecy carries a fearful cost."[192] When this cost meets the dynamics of irregular warfare, the requirements of survival and action generally produces a response that sacrifices elements of speed, technology, and efficiency.[193] This dilemma of secrecy vs. efficiency characterizes the nature of covert communications, and an overall desire to secure communications. Pressure against a network forces constraints on communications, often to the point of tremendous inefficiency. A general pattern that

[192] Bell, "Aspects of the Dragonworld," 23.

[193] Ibid., 26.

emerges is that those in positions of leadership or operational responsibility generally use lower-tech methods of communication to ensure secrecy, while those in operational units, fighters, use high-tech communications, trading an element of secrecy for the flexibility required in operational action. Despite guidance from leadership to avoid these high-risk types of communications, this usage occurs with surprising frequency, as a former international narco-trafficker explains, "there are many who say they never use the phone because it is too insecure. They are either lying or not doing any business."[194] An example of this is the use of couriers by senior leadership, and cellular and Internet technology employed in a more frequent manner by those conducting operations. Overall, clandestine measures are made easier with the advantages of technology that the information age provides, and their omnipresence tends to create more communication between dispersed nodes than would otherwise be the case.

5. Information Strategy

Networks achieve success through their understanding of the information age, and one of the primary dynamics is the increasingly effect of information strategy. It is increasingly apparent that information strategy holds as great an importance in accomplishing many of the same aims as traditional military strategy. Information strategy is a "still-forming phenomenon" that incorporates the many complexities of the information domain, and seeks to provide structure for the information flows that both impact the enemy and strengthen an individual's self.[195] An examination of current conflicts highlights the rise of the information domain in irregular warfare, and in particular, the almost constant interplay of information strategy with traditional military action.[196] It appears that networks seem to understand this well and their operations are closely tied to information operations. The skillful use of information strategy both enhances the application of traditional military means, directly counters the opponent's

[194] Carlo Morselli and Katia Petit, "Law-Enforcement Disruption of a Drug Importation Network," *Global Crime* 8, no. 2 (May 2007): 17; Eilstrup-Sangiovanni and Jones, "Assessing the Dangers of Illicit Networks," 31.

[195] John Arquilla, "Thinking About Information Strategy," in *Information Strategy and Warfare: A Guide to Theory and Practice*, ed. John Arquilla and Douglas A. Borer (New York: Routledge, 2007), 1.

[196] Ibid., 9.

aims, and ensures the network's own moral and will. The role of information strategy holds greater importance for networks than a purely military strategy due a force disadvantage and the information age's defining impact on modern conflict. Frank Hoffman describes this growing trend:

> The informational component of war is increasing in impact. Modern 24/7 news cycles and graphic imagery, combined with the worldwide networks, produce even faster and higher response cycles from audiences around the globe and offer powerful new tools. Advanced methods and ever lower costs allow many insurgent or terrorist groups to communicate directly to their target audiences.[197]

As an example, the strategic communications skill displayed by al-Qaeda continues to empower their jihadist efforts, while the massive amount of battlefield media operations serves to increase morale and recruitment.

A useful way to examine information strategy is by focusing on its internal effects, within the network and the population that may support it, as well as its external effects, against an opponent and their population. Internally, the information strategy of networks seeks to ensure fluid information flow, much as modern professional armies sought to use information technology to enhance command and control and shared situational awareness. However, because public perception is now as central to irregular warfare as the battlefield was in conventional wars, these internal factors have secondary importance to the external aspects. Externally, information strategy is focused on the populations involved, and thus, networks acquire the greatest asymmetric advantage. Those with close ties to the population (local insurgent networks) are able to reach the local audience more effectively, while those with less ties (global terrorist networks, such as al-Qaeda) are able to use an effective information strategy to transcend tradition population-centric notions.[198] In light of these information age dynamics, the following characteristics provide insight into the nature of fighting networks' information strategy.

---

[197] Frank G. Hoffman, "Mind Maneuvers," 1.

[198] Rid and Hecker, *War 2.0*, 139.

a. Information Diffusion

Network designs promote rapid information diffusion, which leads to swift tactical innovation and shared inspiration, increasing collective intelligence. The information revolution has impacted nearly every aspect of warfare, "but changes in telecommunication have an even more revolutionary impact on irregular forces."[199] The overall information flow within a network is enhanced by information technology, providing for enhanced communication within the network. The primary factor contributing to this greater capability is the dispersion of cellular and Internet-based technology, providing nearly every individual the means to communicate. This increased communications capability allows for further decentralization and autonomy and an increase in the speed of information transmission. The former provides for more innovation and action, and the later ensures that learning is shared in a rapid manner. Innovation is further decentralized as communities of interest are connected by new technology, and challenges are realized and reacted to at the lowest levels.[200] This information and its accessibility is a key feature in what Robb calls, "open-source warfare," or the idea that open collaboration with a common focus provides efficiency and innovation despite its lack of control. One of the primary features of this model is the idea of a bazaar, or a robust, open marketplace that facilitates information sharing and develops innovation.[201] However, this increased ability must be balanced with the requirement for security, always a primary consideration, which necessitates compartmentalization and restrictions on communication.

In addition, information technology provides the means to spread ideas rapidly and inspire a cause. Networks utilize their dispersed structures to further connections with numerous sources. This ability to form external connections is a tremendous advantage of the network structure. This external outreach, coupled with the information revolution, provides networks with the means to influence the population to a greater degree than previously thought possible. In fact, in many instances, the evolution

---

[199] Rid and Hecker, *War 2.0*, 13.

[200] Ibid., 31.

[201] Robb, *Brave New War*, 118.

in information technology provides terrorists and insurgents the means to create and broadcast their message in ways not only much faster than traditional media, but that bypass it altogether.[202] The Internet is the principle forum for this external communication and it provides the ability to link dispersed segments of the global population. Currently, all major terrorist and insurgent networks have their own Web sites, and many have the ability to regenerate sites rapidly when they are shut down.[203] Al-Qaeda and other networks utilize autonomous messaging and communication forums and reach out to dispersed audiences in a manner that enhances their appeal through tribal norms of communication.[204] The Zapatista Movement in Mexico provides a compelling example for the power of networked communication as a dedicated focus. The Zapatista's utilization of mass media and Internet connectivity to achieve social awareness provides the seminal example of information-centric conflict, and became the compelling force in their movement.[205] As the Zapatistas leader and spokesman, Subcomandante Marcos called for a "network of information," his ideal of the "word" as a weapon became a reality and displayed the power of a modern information strategy for a resistance movement.[206]

b. Information Strategy Determines Operations

Networks conduct operational activity to influence popular perceptions, which requires a close synchronization with information strategy. Despite differences in types of irregular warfare, and the motivations that drive networks in their asymmetric fights, public perception plays a greater role in netwar than in traditional warfare. The primary focus in irregular warfare is insurgency, which describes a type of warfare generally waged by people with grievances, and which has a political objective. As

---

[202] Hoffman, *Inside Terrorism*, 198.

[203] Ibid., 206.

[204] Ronfeldt, "Al-Qaeda and its Affiliates," 42.

[205] David Ronfeldt and John Arquilla, "Emergence and Influence of the Zapatista Social Netwar," in *Network and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David F. Ronfeldt (Santa Monica, CA: RAND, 2001), 190.

[206] Subcomandante Insurgente Marcos, *Our Word is Our Weapon: Selected Writings*, ed. Juana Ponce de Leon (New York: Seven Stories Press, 2002), 181.

Robert Taber states in *War of the Flea*, "successful insurgency presupposes the existence of valid popular grievances, sharp social divisions, an unsound or stagnant economy, an oppressive government."[207] Insurgencies take several forms, including wars of national liberation against an oppressive power, internal revolutionary struggles, and conflict waged by minorities to achieve various ambitions.[208] An insurgent network is closely tied to the goals and aims of the people who support its formation, and seeks to convince the population that it is a better model for governance and security.

The other focus in irregular warfare is terrorism, a tactic employed in a military manner to influence popular perception in insurgencies, but which may also be employed for primarily ideological ends as well. Networks that utilize terrorist tactics, especially against their own population, are generally less connected to, or dependent on popular support. While insurgencies may use terror tactics, they do so at the risk of alienating the very population they are seeking to influence. Still, terrorist networks seek to influence popular perception through their tactics, as terrorism uses violence against victims to influence a target audience. This target audience may be the local population, but in most instances, it is the existing government or external power influence.

The underlying theme in the crafting of information strategy is the story, or what Sageman describes as the "grand narrative."[209] Arquilla and Ronfeldt address this aspect in detail with their use of the narrative framework, which is intimately linked to social connections.[210] The narrative serves as a "rough guide to action, informing cadres whom they should attack and encouraging the rise of self-synchronized actions by the many who come under no one's direct control."[211] In this sense, fighting networks are guided by their information strategy, and proactively seek out and design operations to gain advantages in the information realm. Professional militaries, and even traditional irregular opponents, utilize information strategy primarily as a reactive measure, to

---

[207] Taber, *War of the Flea*, 151.

[208] Chaliand, *Guerrilla Strategies*, 11.

[209] Sageman, *Understanding Terror Networks*, 144.

[210] Arquilla and Ronfeldt, *Networks and Netwars*, 324.

[211] Arquilla, *Aspects of Netwar and the Conflict with Al-Qaeda*, 2009, 5.

mitigate and influence effects from military actions.[212] In contrast, networks understand the inherent power of the information age and utilize narratives as an over-arching weapon.[213]

c. Intelligence

Networks require a high degree of intelligence, and its systematic use determines their operational tempo. In an effort to achieve their goals, networks place considerable emphasis on intelligence collection and planning, ensuring that they minimize their chances of failure and maximize success. Intelligence superiority is a fundamental attribute of irregular opponents attacks, describing the process of selecting targets, gathering information to aid in operational planning, analyzing weaknesses, and ultimately, providing the attacker with the greatest chance of success. In addition, in many cases, terrorists emphasize good intelligence not only to ensure mission success, but also their own survival, a critical factor with small numbers.[214] While conventional military forces use intelligence as well, it is traditionally of secondary emphasis to the value of sheer maneuver.[215]

Classically, intelligence provides irregular opponents with the information to anticipate an opponent's movement, decipher intentions, and most importantly, identify weaknesses. In describing the challenges of intelligence in irregular warfare, Gregory Treverton argues that terrorists take intelligence in a different direction. Rather than simply a case of mirror-imaging analysis of an opposing force, terrorists shape their "capabilities to our vulnerabilities," and conduct detailed reconnaissance to identify vulnerabilities, which then form the basis for planning.[216] The vast quantities of information available using open sources, such as those on the World Wide Web, provide

---

[212] Rid and Hecker, *War 2.0*, 35.

[213] Ibid., 128–129.

[214] Hoffman, *Inside Terrorism*, 249.

[215] David Kahn, "A Historical Theory of Intelligence," in *Intelligence Theory: Key Questions and Debates*, ed. Peter Gill, Steven Marrin and Mark Pythian (New York: Routledge, 2009), 5–10.

[216] Gregory F. Treverton, *Intelligence for an Age of Terror* (New York: Cambridge University Press, 2009), 5.

a virtual and expansive library. Gabriel Weimann's comprehensive work, *Terror on the Internet*, describes the collection of this information as "data mining," and describes extensive research, information sharing using online forums, and al-Qaeda cells with "'large databases containing details of potential targets in the U.S.'"[217] The vast amount of information that provides for everyday convenience imparts details for identifying weaknesses and serves as access for attack planning. While decentralization may limit information stockpiling and sharing, because such networks rarely have a central directory for cataloging and referencing information, most of the "usable" information they require is readily available.[218]

d. Information Asymmetry

Networks use modern information technology, in ways that complement their design, to achieve a strategic information advantage relative to their opponents. The proliferation of information technology in increasingly powerful forms, with greater availability, ensures that networks are as equipped with the means to communicate on the strategic level as their opponents. These technological tools increase capability, but the greater factor is the overall understanding of the importance of the possibilities that the information age provides. Thomas Rid and Marc Hecker describe six informational asymmetries that extend from the basic dynamics of irregular warfare.

1. The counterinsurgent is bound by the truth; the insurgent is not
2. The show of violence tends to benefit the insurgent; it damages the counterinsurgent
3. In the media sphere, the insurgent has the initiative while the counterinsurgent reacts
4. Anonymity benefits the insurgent while it harms the counterinsurgent
5. The costs or media operations rise for the counterinsurgent while falling for the insurgent

---

[217] Description of al-Qaeda databases from Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism* (New York: McGraw-Hill Osborne Media, 2003); Gabriel Weimann, *Terror on the Internet* (Washington, DC: United States Institute of Peace Press, 2006), 112.

[218] Eilstrup-Sangiovanni and Jones, "Assessing the Dangers of Illicit Networks," 19.

6. Modern information technology—by and large—increases risks for the counterinsurgent; it decreases risk for the insurgent[219]

While these asymmetries are framed in classic insurgency terms, they generally apply to many aspects of strategic information employed by networks. The first two are timeless, but the last four are either greatly enhanced or derive directly from the use of modern information technology. From the standpoint of initiative, a network's ability to access mass media through modern data platforms allows it the ability to "flood" the presses, while those who oppose it must analyze, verify, synchronize and then respond. Likewise, anonymity is greatly increased by the ability to simply place messaging in the public sphere, either through a media outlet, or directly through unilateral media. In addition, increasing accessibility of information technology and communications platforms results in less cost for networks, even allowing superiority in real-time strategic communications. Finally, networks acquire a strategic information advantage because the modern tools of information technology pose less physical risk. It is far easier to erase electronic media on a commonplace system than it is to destroy a clandestine printing press. Overall, these asymmetries point towards increased violence, as is seen by a rapid acceleration in terror attacks. While these attacks are highly visible, networks exhibit more clandestine behavior, but despite this anonymity, successfully foster a significant media presence.

D. NETWORK-STYLE WARFARE

Fighting networks represent a form of warfare that is truly a paradigm shift, and that reflects the revolutionary changes of the information age. These networks utilize timeless principles of irregular warfare, but are defined by unique organizational forms, doctrine, operational methods, and use of information strategy. The combined characteristics of each of these areas provide an overall understanding of how networks fight.

[219] Rid and Hecker, *War 2.0*, 131–132.

1. Characteristics

a. Organizational Attributes

1. Networks are structurally characterized by high levels of decentralization, which allows for autonomous action and high degrees of operational initiative.
2. Networks fight with synchronized nodes, or cells, which provide advantages in tactical control and security.
3. Irregular warfare is dynamic and networks achieve resiliency through unique organizational structures.
4. Effective networks are flexible, adapting their structure to the environmental conditions, which makes them resistant to any one form of pressure.
5. Networks form primarily through trust-based relationships, which sustain high-risk activity and provide operational advantages.
6. Networks rarely rely on direct command and control, which provides flexibility and autonomy in tactical decision making, but may decrease collective direction.

b. Doctrine

1. Networks fight using a unique, combined doctrine, which blurs offensive and defensive attributes.
2. Networks utilize swarming as a fundamental aspect of their doctrine, and one that provides a distinguishing element from other forms of irregular war.
3. Networks are capable of fighting in a protracted manner, but take the initiative when it presents itself, demonstrating staying power, but also seizing on opportunities for rapid victory.
4. Networks rely heavily on deception, in the form of concealment, to ensure favorable conditions from the tactical through strategic levels.
5. Networks attack weakness using systems disruption, in addition to directly confronting an opponent's forces.

c. Operational Methods

1. Networks generally lack resources compared to their opponents, but being lightly armed provides multiple operational advantages.

2. Networks display a high degree of stealth, which is a fundamental attribute of their tactical decision making.
3. Networks require surprise, which provides the decisive element in attacks against stronger opponents.
4. Networks require clandestine mechanisms to maintain secrecy, but these can create operational inefficiencies.

d. Information Strategy

1. Networks promote rapid information diffusion, which leads to swift tactical innovation and shared inspiration.
2. Networks conduct operational activity to influence popular perceptions, which requires a close synchronization with information strategy.
3. Networks require a high degree of intelligence, and its systematic use determines their operational tempo.
4. Networks use modern information technology to achieve a strategic information advantage relative to their opponents.

The organizational frame provides the dominant aspect for understanding how networks fight, and why network-based operations are considered a unique aspect of irregular warfare. Composed of numerous small elements, from the group to individual level, networks are fundamentally decentralized. This decentralization ensures a high level of autonomy, which provides tremendous initiative and allows these small elements to maneuver with significant stealth, maximizing both speed and concealment. Small elements favor increased control at the tactical level, and greater security overall. In addition, networks achieve a significant degree of resiliency through their organizational structure, as well as their ability to vary their operational activity to ensure organizational survival. This resiliency stems from their organizational flexibility, responding to changes in the environment, and ensuring that all aspects of their war-fighting systems flex as well. Finally, networks primarily form through trust-based relationships, utilizing friendship and kinship ties in ways that are more suggestive of basic cultural forms, such as clans and tribes. These strong ties sustain high-risk activity and provide operational advantages.

These organizational characteristics are inherently tied to network doctrine, which provides a framework and common principles for irregular warfare. The

central role of the population in irregular warfare is the most significant feature, which characterizes doctrine. Irregular warfare further emphasizes the expression of war as the continuation of politics by other means, and it provides for a unique blend of doctrine. This doctrine blurs the lines between traditional forms of doctrine, such as offense, defense, and deterrence in ways expressed in a mix of strategic through tactical aspects. Popular will is as important as military force, and networks may prolong conflict as a means of demonstrating superior will, or may seek rapid and decisive victory. Deception forms a significant element of network doctrine, just as it does in guerrilla warfare, and it stems from the hider-finder dynamic produced by force asymmetries. Another aspect of asymmetry in irregular warfare is the doctrine of attacking weakness through systems disruption rather than directly confronting superior forces. This form of indirect strategy is increasing utilized as the information age provides greater connectivity and exposure of vital systems.

Just as organization influences doctrine, and vice versa, the operational methods displayed by networks are more of a system of operations than rigid procedures. Networks are generally lightly armed, but utilize this characteristic to provide powerful advantages, which demonstrates that resources are not a determining factor in how they fight. One of the advantages that being lightly armed provides is the ability to achieve a high degree of mobility relative to their larger, heavily resourced opponents. This mobility is usually expressed in the form of stealth, and characterizes nearly every tactical decision, from infiltration to withdrawal. Stealth enables one of the primary aspects of network doctrine, the swarm, demonstrating the superiority of this characteristic over traditional principles, such as mass and firepower. Swarming, and nearly every operational characteristic of networks, is enhanced by the principle of surprise. While surprise is not unique to irregular warfare, networks require it to gain advantages over their opponent’s superior force, and it exceeds the importance of sheer maneuver. Operationally, nearly every aspect of war fighting is influenced by the requirement to maintain some level of secrecy, which creates inefficiencies in their ability to operate.

Networks display a fundamental understanding of information age impacts on irregular warfare; in fact, this attribute provides the most dramatic aspect of their evolution. The revolutionary dynamics of information technology influence each aspect of how networks fight, but it is most readily apparent in their use of information strategy. Internally, their use of information technology promotes rapid information diffusion, which creates innovation and inspiration. Their operational cycle flows from a requirement for intelligence, which in turn, is synchronized with media operations designed to influence popular perceptions. These popular perceptions drive an external information strategy that uses the advantages of modern information technology to produce asymmetrical advantages.

Each of these aspects of analysis provides insight into how networks fight and their synchronized effects illustrate the overall effectiveness of network-based operations. Networks fight differently than professional western armies, but they also use a synthesized system of characteristics that provide for a unique method of fighting. Rather than follow Clausewitz and other strategists who focus on set-piece battles, networks are much more in line with Sun Tzu, and focus on indirect strategy, guerrilla warfare, and deception. In the chaos of irregular warfare, networks seek to promote friction in their opposing forces, rather than attempting to minimize their own. While using modern information technology, they are not necessarily constrained by it. In contrast to larger conventional militaries, they exhibit a high degree of flexibility, which begins at the organizational level, but influences every characteristic of their war fighting. While the origins of irregular warfare stretch back to the beginning of conflict, networks transcend much of the traditional techniques of unconventional warfare with an information age awareness that results in an unprecedented threat.

2. Strengths and Weaknesses

The strengths and weaknesses displayed by fighting networks are based on the previous collection of characteristics, as well as a holistic understanding of irregular warfare. Some overlap exists in strengths and weaknesses, recognizing that this trait is common in organizational aspects, doctrine, and even physical systems. In many ways,

these characteristics provide a double-edged sword and the capabilities they describe both empower and emperil. Generating strengths and weaknesses is a critical step in developing an understanding of an opponent and provides the initial basis for understanding critical vulnerabilities for targeting.

a. Strengths

- Decentralization provides greater autonomy in the realm of conflict, which allows for more operational initiative and self-synchronization.
- The less directive role that leadership plays means that the network is less reliant on direct control.
- Linked nodes allow synchronized tactical control and greater security in the form of concealment and compartmenting.
- Network structures are more resilient to outside pressures, and often utilize multiple network forms in combination.
- Network structures provide greater flexibility with respect to changing environmental conditions than hierarchies.
- Networks achieve strength through trust-based relationships, which sustain high-risk activity and increase operational effectiveness.
- A network's ability to achieve concealment among the population and/or terrain is a tremendous advantage.
- Lightly armed elements allow for greater stealth, providing advantages in mobility and concealment.
- Networks use information technology to achieve an advantage in strategic communications.
- Information technology allows networks to mobilize, train, recruit, and finance with little cost and wide access.

b. Weaknesses

- Decentralization makes it difficult to exert control over operations, as well as enforce security measures.
- Small nodes are at a tremendous disadvantage without surprise at the tactical level, which is achieved through concealment-oriented deception.
- Network structure provides for a great degree of resiliency, but it is more prone to total collapse if a significant amount of hubs fails.

- Networks are limited by their ability to achieve a balance between persistence and operations.
- Trust-based relationships provide a means to identify network actors, as well as a potential point of fracturing.
- All-channel connections increase the potential for infiltration into the network.
- Networks must prepare to fight for a long duration, balancing decisive victories with an ability to persist.
- The requirement for secrecy requires clandestine mechanisms, which create communication inefficiencies.
- Operational tempo is limited by intelligence because raids and ambushes, and even swarming, require it in significant amounts.
- Networks are increasingly reliant on public information technology—it both sustains and imperils.

Examining both strengths and weaknesses reveals the impact of significant network commonalities, notably the important role of organization and information. Among the strengths, high levels of autonomy and decentralization generate swift operational action, but also create difficulties in forming consensus and coordinating complex actions. Organizational aspects provide the greatest impact of both strengths and weaknesses, but the role of information is not far behind, as its skillful employment provides significant capability for inherently weaker networks.[220] Information also has a unique relationship with a network's ability to remain concealed. On the one hand, those seeking to counter networks must possess the information necessary to find network nodes, while fighting networks strive to contain such information. In contrast, networks much continue to be visible and active in the information domain, for both strategic advantage and operational utility.

E. CONCLUSION

A general consensus exists that the idea of networks provides the most descriptive means of identifying the irregular opponents that challenge security and stability globally. "Since the attacks [9/11], we have become accustomed to the idea that the West is battling against a decentralized 'network of terrorist cells' that lacks any hierarchical command structure and is distributed throughout the world."[221] However, despite this

[220] Rid and Hecker, *War 2.0*, 134–136.

[221] Buchanan, *Nexus*, 21.

growing awareness, much of the traditional methods of irregular and even traditional warfare continue to be employed to counter these networks. Fighting networks are the defining feature of modern irregular warfare, usually combining elements of guerrilla warfare and terrorism in ways that defy traditional analysis. Their utilization of unconventional fighting techniques and modern information technology demonstrates a revolutionary change from traditional insurgencies and unconventional warfare, and is now the defining challenge of conflict in the information age. These networks are increasingly empowered, and their ability to challenge nation states, despite their professional militaries, has significant implications. This analysis of fighting networks reveals that while they share features with their social network counterparts, these networks are redefining warfare.

Networks include both insurgent and terrorist threats and utilize multiple aspects of irregular conflict, as the U.S. State Department's 2003 Global Patterns of Terrorism described how the "line between insurgency and terrorism has become increasingly blurred."[222] This blurring requires a new paradigm that goes beyond traditional definitions, and the key differences between network-style warfare and traditional guerrilla warfare highlight the requirement for the netwar paradigm. While networks incorporate some aspects of guerrilla warfare, they are different from classic guerrilla organizations, and reflect information age dynamics in organization, technology, and strategic outlook. Advances in modern information technology enable flattened, empowered organizational structures and innovative operational methods. While technology provides the tools that enhance many of the classic methods of irregular warfare, it is simply a tool, and the most significant aspects are the ways in which this technology is applied. As seen in the distinction between NCW and netwar, the use of technology is not indicative of effectiveness, nor is the quantity or quality. Instead, the incorporation of organization, doctrine, operational methods, and information strategy

[222] U.S. Department of State, Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism*, 2003, 113, http://www.state.gov/s/ct/rls/crt/2003/index.htm.

provides a cohesive application, and results in achieving an effective system. The characteristics these lenses present synchronize into a coherent framework describing the ways networks fight, and revealing their strengths and weaknesses.

III. HOW TO FIGHT NETWORKS

> Victory in war is not repetitious, but adapts its form endlessly….The ability to gain victory by changing and adapting according to the opponent is called genius.[223]
>
> –Sun Tzu

A. FACING A NETWORK THREAT

The fighting networks of the 21st century present a fundamentally different challenge than that posed by traditional militaries and classic irregular opponents. These networks leverage modern information technology to create new connections and possibilities in conflict that result in increasingly formidable opponents bringing change to warfare. Warfare in the information age poses significantly different threats, increasing in complexity and capability, which are best described by their network form. As Thomas Hammes describes these changes, modern warfare is utilizing, "all available networks—political, economic, social, and military—to convince the enemy's political decision makers that their strategic goals are either unachievable or too costly for the perceived benefit."[224] The traditional approach to war that simply assumes facing off against another professional military operating with a similar doctrine and similar technological advantages is increasingly less relevant. Given the unique advantages that networks gain through their synchronization of war-fighting techniques in the information age, it is clear that they pose significant challenges in the modern era.

While a general survey of irregular warfare reflects multiple examples of irregular fighters successfully challenging nation-states, the rise of modern fighting networks presents an even greater challenge. Recent history shows irregular opponents to be increasingly successful in their efforts to counter professional militaries successfully. The Afghan *mujahedin* efforts to counter the Soviet Union in the late 1980s provide a clear

---

[223] Sun Tzu, *The Art of War*, 101.

[224] Thomas X. Hammes, *The Sling and the Stone: On War in the 21st Century* (St. Paul, MN: Zenith Press, 2004), 2.

example of a guerrilla organization that forced a nation-state's withdrawal from their country. Another notable example is the Habr Gedir clan that forced the U.S. withdrawal from Somalia in 1993.[225] In 2000, Hezbollah, using classic guerrilla tactics and terror strikes against Israeli forces and their Lebanese proxy militia likewise forced them out of southern Lebanon.[226] More recently, the examples of professional militaries frustrated by insurgent and terrorist networks in Iraq and Afghanistan highlight the further empowerment of modern networks. After nearly a decade of war in Afghanistan, an international coalition of the most advanced military forces is still fighting an opponent with no army, navy, or air force, which clearly demonstrates the existence of factors beyond technological advantages and superior force levels. Moreover, a blend of network-style warfare, cutting-edge weapons and information capabilities provides more advanced non-state networks, such as Hezbollah, with tremendous capability. Fighting networks are increasingly empowered, and it is likely that the next major confrontation with such a network will present even greater challenges than those posed in current conflicts.

Modern militaries tend to focus primarily on countering traditional opponents, which fight in a similar manner, only occasionally facing irregular and "revolutionary" opponents, as evidenced during the post-colonial period. However, despite the dramatic increase in irregular and low-intensity conflict, these wars are viewed as a sideshow to larger traditional warfare. The proliferation of insurgencies and an increase in terrorism throughout the globe brought numerous attempts to counter irregular opponents. However, while insurgency has been the most common form of armed conflict since World War II, professional militaries remain focused on traditional confrontations with similar opponents.[227] In general, nation-states have a mixed record in facing the challenges presented by non-state actors, and even success has often carried a serious price. In addition, successes, such as that gained by Army Special Forces (SF) teams in

[225] Shultz, Jr. and Dew, *Insurgents, Terrorists, and Militias*, 86–100.

[226] Judith Palmer Harik, *Hezbollah: The Changing Face of Terrorism* (New York: I.B. Taurus & Co. Ltd., 2004), 125–145.

[227] Thomas X. Hammes, "Why Study Small Wars?" *Small Wars Journal* 1 (April 2005).

countering the Taliban in 2001, employed "another kind of war—guerrilla-style/light-footprint/culture-centric and low-intensity," whose gains were lost as the coalition reverted to a traditional warfare approach.[228] Irregular war poses different dilemmas and military strategy wrestles with the dissonance created between the customary focus of fighting a similar foe to dealing with an irregular opponents. Some would argue that the risks associated with failure against another peer or near-peer adversary are much greater than that associated with failure against irregular opponents, necessitating a primary focus on major combat operations.[229] However, in the same study of the 30 most recently resolved insurgencies from 1978–2008, all but eight resulted in losses for the "superior" nation-state COIN forces.[230] This record, combined with the increasing empowerment of fighting networks, requires a more adaptable approach—one suitable to the changing nature of irregular conflict in the information age.

As the information age progresses, pronounced aspects of the spectrum of conflict become clearer, with irregular threats presenting greater challenges. Just as nation-states struggled with the emergence of revolutionary war in the last century, the threat posed by fighting networks presents further challenges in contemporary warfare. Modern strategy shows that the Western powers embrace technological changes rapidly, but modify doctrine much more slowly, and "learning to cope with a very different kind of warfare, in which words do more to mask or distort military reality than to reveal it, has proved far more difficult."[231] Revolutionary warfare and dramatic technological changes ushered in an era defined by a revolution in military affairs, but threats are evolving as well, leaving modern militaries searching for ways to counter irregular opponents. Current U.S. military doctrine recognizes these changes in irregular warfare, but perhaps not as fully as required:

---

[228] Doug Stanton, *Horse Soldiers* (New York: Scribner, 2009), 367.

[229] Christopher Paul, Colin P. Clarke and Beth Gill, "Victory Has a Thousand Fathers: Evidences of Effective Approaches to Counterinsurgency, 1978–2008," *Small Wars Journal*, 8, http://www.smallwarsjournal.com.

[230] Paul, Clarke and Gill, "Victory Has a Thousand Fathers: Evidences of Effective Approaches to Counterinsurgency, 1978–2008," 12.

[231] John Shy and Thomas Collier, "Revolutionary War," in *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, ed. Peter Paret (Princeton, NJ: Princeton University Press, 1986), 821.

> Faced with the conventional warfighting capacity of the United States, our adversaries will likely choose to fight using a hybrid of irregular, disruptive, catastrophic and traditional capabilities as a way to achieve their strategic objectives. The strategy of our adversaries will be to subvert, attrite, and exhaust us rather than defeat us militarily. They will seek to undermine and erode the national power, influence, and will of the United States and its strategic partners.[232]

The primary aspect of this threat is that opponents of all types will use other than traditional military means, but still seek to defeat the United States in conflict. The Chinese military theorists, Qiao Lang and Wang Xiangsui, in their work, *Unrestricted Warfare*, highlight the growing trend of those who recognize force asymmetry, but seek to gain advantages by networking combinations military and nonmilitary power in new ways. They see warfare itself as being in the midst of dramatic change, as the "new principles of war are no longer "using armed force to compel the enemy to submit to one's will,'" but rather are "using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests."[233] Qiao and Wang highlight the effects of the "most important revolution in the history of technology," modern information technology, and show how it presents the means to transcend traditional notions of warfare with numerous non-war actions that "may be the new factors constituting future warfare."[234] They call this unrestricted warfare, and state that:

> This kind of war means that all means will be in readiness, that information will be omnipresent, and the battlefield will be everywhere. It means that all weapons and technology can be superimposed at will, it means that all the boundaries lying between the two worlds of war and non-war, military and non-military, will be totally destroyed, and it also means that many of the current principles of combat will be modified, and that even the rules of war may need to be rewritten.[235]

---

[232] U.S. Department of Defense, *Irregular Warfare Joint Operating Concept*, Version 1.0 (Washington, DC: U.S. Joint Chiefs of Staff, January 2007), 15–16.

[233] Qiao Lang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), 4 http://www.cryptome.org/cuw.zip.

[234] Ibid., 6.

[235] Ibid., 6–7.

Unrestricted warfare stems from the advances and interconnectivity that the information age provides, and combines multiple aspects of warfare in a networked style. Fighting networks herald this style of unrestricted warfare, clearly recognizing force asymmetry but also the advantages the information age presents by enabling new forms of organization, doctrine, methods, and information strategy. Displaying every aspect of unrestricted warfare, increasingly empowered networks successfully confront nation-states and deny them their objectives. A notable example is the confrontation between Israel and Hezbollah in 2006, and it is widely believed that future irregular conflicts will continue to be asymmetric, but will increase in complexity and intensity.[236] As fighting networks grow stronger, empowered by increasingly sophisticated technologies and perhaps with weapons of mass destruction, once available only to an exclusive group, the damage inflicted by confrontations with these rogue opponents may be much greater, and pose an existential risk to nation-states.

The emergence and increasing empowerment of insurgent and terrorist fighting networks, and the trend in irregular warfare that they represent, call for an effective way to counter these networks. This section provides the basis for a theory on countering fighting networks. The initial portion of this endeavor is based on the ways in which networks fight, and draws from the primary strengths and weaknesses they exhibit. These strengths and weaknesses are evaluated for vulnerabilities. These vulnerabilities are then examined in the context of irregular warfare to develop counter-network hypotheses leading to a set of variables that should provide for effective counter-network operations. As an intermediate evaluation of these variables, prior to being tested by each of the case studies, they are examined using four different models of warfare employed against fighting networks. The degree to which these models address the specific variables provides an indication of how instrumental they will be in an effective counter-network strategy. This process produces a proposed theory for countering fighting networks, one based on network vulnerabilities and evaluated against four common models.

---

[236] Nathan Freier, *Small Wars 2.0: A Working Paper on Land Force Planning After Iraq and Afghanistan* (Carlisle Barracks, PA: U.S. Army Peacekeeping and Stability Operations Institute, 2011), 4, http://pksoi.army.mil/PKM/publications/relatedpubs/documents/Small_Wars_2.0.pdf.

B. COUNTERING NETWORKS

1. Counter-Network Literature

An increasing realization of the threat from fighting networks and a growing field of study is occurring, which seeks to develop ways in which to understand these networks. Much of this literature is focused on analyzing network structure using social network analysis tools to determine various aspects of the network.[237] A notable study in this group is "Destabilizing Networks," by Kathleen Carly et al., which provides insights beyond centrality measures and addresses significant factors, such as cognitive load, while seeking to address "large, adaptive, multi-plexed, multi-coloured networks, with high levels of missing data."[238] These descriptive approaches generate significant analysis of specific network aspects and hold great promise as tools within the development of a comprehensive approach to countering networks. A few other studies have addressed the idea of counter-network warfare, but usually in ways that focus more on strategic discussions.[239] Overall, though, little is still written that may provide an effective concept and methodology for effectively countering fighting networks within irregular warfare.

The most commonly discussed operational approach to countering fighting networks is COIN, under the assumption that most irregular threats consist of guerrilla with insurgent aims, which fills most of the irregular warfare field of study. The recent

---

[237] See, for example, Krebs, "Mapping Networks of Terrorist Cells," 43–52, 2001; Kathleen M. Carley, Ju-Sung Lee, and David Krackhardt, "Destabilizing Networks," *Connections* 24, no. 3 (2002): 79–92; Jose A. Rodriguez, "The March 11th Terrorist Network: In Its Weakness Lies Its Strength," Presented at Sunbelt XXV: International Sunbelt Social Network Conference, February 16–21, 2005, Redondo Beach, CA; Sageman, *Understanding Terror Networks*; Raab and Milward, "Dark Networks as Problems"; Ian S. Davis, Carrie L. Worth, and Douglas Zimmerman, *A Theory of Dark Network Design* (Master's thesis, Monterey, CA: Naval Postgraduate School, 2010).

[238] Carley, Lee, and Krackhardt, "Destabilizing Networks," 90.

[239] Much of the strategic focus addresses the changing nature of terrorism, such as Ian O. Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt, Michele Zanini, *Countering the New Terrorism* (Santa Monica, CA: RAND, 1999); Spulak, Jr. and Turnley, "Theoretical Perspectives of Terrorist Enemies as Networks." Other studies place more emphasis on the changing nature of warfare, primarily focusing on networks in unrestricted warfare. See, for example, the collection of articles in the *Proceedings of the Unrestricted Warfare Symposium*, published yearly 2006–2009, http://www.jhuapl.edu/ourwork/nsa/projects.asp.

confrontations against violent networks in Iraq and Afghanistan are described as insurgencies, as are most popular-based uprisings.[240] However, counter-insurgency may not provide the best perspective for facing all networked-based threats, being ill-suited to addressing fighting networks that may not require, or seek, popular support. "Modern insurgencies tend to be loose coalitions of varied political tendencies. Correspondingly, their structure takes the form of a decentralized, even loose, network rather than a hierarchical organization."[241] In addition, fundamental assumptions of counter-insurgency are based on countering a guerrilla threat; which is increasingly less true as networks embrace high-intensity warfare. Another approach commonly referenced is the use of CT techniques employed to counter the rise of modern terrorist organizations successfully in the 1970s and 1980s. However, these basic counter-terrorism models may not be adequate, primarily, because the nature of the threat is more complex, or has changed dramatically enough that most of the literature no longer fits. Moreover, in the quest to find ways to counter these networks, beyond just COIN or CT, some literature addresses both, or highlights the merits of one approach over the other.[242] A growing recognition of the importance of networks exists, as both the current COIN and CT doctrinal manuals are beginning to address network aspects and analysis.[243] However, a significant void does exist in both formal doctrine and irregular warfare studies in discussing highly adaptive irregular threats that employ neither classic guerrilla warfare nor just terrorism. Still, the focus on irregular threats within these areas provides further understanding of the principles governing irregular warfare and practices, which may be

---

[240] The field of counter-insurgency study is both broad, describing such efforts throughout time, as well as deep in its current discussions and debates. Notable works reflecting the breadth of study were described in Chapter I, while some of the more recent articles include: David Kilcullen, "Counter-Insurgency Redux, *Survival* 48, no. 4 (2006): 111–130; T. F. Lynch III, "Conceptual and Operational Challenges of COIN: Executive Summary," *Joint Forces Quarterly* 60, no. 1, National Defense University Press, 2011. http://www.ndupress.ndu.edu; John P. Sullivan and Adam Elkus, "Strategy and Insurgency: An Evolution in Thinking?" http://www.opendemocracy.net.

[241] Gordon Hahn, "The Jihadi Insurgency and the Russian Counterinsurgency in the North Caucasus," *Post-Soviet Affairs* 24, no. 1 (January–March 2008): 2, http://bellwether.metapress.com/content/90vpnp3464h5243h/fulltext.pdf.

[242] Michael J. Boyle, "Do Counterterrorism and Counterinsurgency Go Together?" *International Affairs* 86, no. 2 (2010): 333–353, Blackwell Publishing, Ltd.

[243] U.S. Department of Defense, Field Manual 3-24, *Counterinsurgency* (Washington, DC: U.S. Government Printing Office, 2006); U.S. Department of Defense, Joint Publication 3-26, *Counterterrorism* (Washington, DC: U.S. Government Printing Office, 2009), II–12—II–13.

effective. These principles from COIN and CT provide additional background, context, and insight by suggesting ways in which irregular threats may be countered, and aid in developing hypotheses to counter fighting networks.

2. Developing Counter-Network Theory

Although the study of irregular warfare stresses the nature of its challenges, it is clear from the ways networks fight that they have both strengths and weaknesses. These aspects may be identified and countered. This effort to disrupt networks directly is essential, despite the challenges of ambiguity and complexity, but must also be synchronized with constructive efforts, such as Kilcullen's proposal of friendly parallel networks.[244] Carley et al. describe how it is difficult to destabilize decentralize, distributed networks, but provide three indicators of what destabilization would look like, including a reduced rate of information flow, difficulty in reaching overall consensus, and less effectiveness in overall task performance.[245] U.S. military doctrine specifically identifies the threats posed by these networks in irregular warfare, and asserts that critical vulnerabilities may be targeted:

> Our enemies may be loosely organized networks or entities with no discernible hierarchical structure. Nevertheless, they have critical vulnerabilities to be exploited within their interconnected political, military, economic, social, informational, and infrastructure systems. These actors often wage protracted conflicts in an attempt to break the will of the nation-state. Military operations alone rarely resolve such conflicts.[246]

While this general statement provides little detail, other doctrinal manuals reinforce this overall view, stating that "a 'networked enemy' has certain vulnerabilities that can be exploited," and "perturbations of nodes in the network may present opportunities for intelligence collection and/or allow more effective isolation. Networked enemies have

---

[244] David Kilcullen, "Build It and They Will Come,"—Use of Parallel Networks to Defeat Adversary Networks," in *Proceedings on Strategy, Analysis, and Technology*, ed. Ronald R. Luman, Unrestricted Warfare Symposium, 2006, 275, http://www.jhuapl.edu/ourwork/nsa/projects.asp.

[245] Carley, Lee, and Krackhardt, "Destabilizing Networks," 90.

[246] U.S. Department of Defense, Joint Publication 1, *Doctrine for the Armed Forces of the United States*, I–1.

different vulnerabilities than hierarchical enemies."[247] An examination of the strengths and weaknesses of fighting networks identified in the previous section reveals a combination of factors that may create vulnerabilities, or opportunities to disrupt networks. One of the insights is that some of the same characteristics that provide advantages to networks also serve as potential vulnerabilities, a characteristic that is true of most organizational forms. For example, organizationally, decentralization provides for greater autonomy and more operational initiative, but it presents difficulties in overall operational control and security. Small nodes provide for advantages in tactical control and concealment, but their force limitations require the use of deception and a reliance on attack with the element of surprise. In this regard, while it may appear that countering networks is simply a matter of attacking weaknesses, the primary focus must be on the vulnerabilities that various characteristics provide. Using the strengths and weaknesses drawn from examining how networks fight, this portion of the study derives a set of network vulnerabilities. These primary vulnerabilities are the following.

- The decentralized nature of networks provides for great initiative but may be countered by similar units using offensive swarming. (Organization/Doctrine)
- Complex synchronization among multiple decentralized units requires overarching purpose and extensive communication. (Information Strategy/Organization/Doctrine)
- Networks are reliant on their ability to conceal themselves. (Doctrine)
- Free-scale network structure provides resiliency and flexibility, but is vulnerable to a concerted attack against its hubs. (Organization)
- Strong ties based on trust provide a means to identify and "unravel" the network. (Organization)
- Clandestine mechanisms preserve network secrecy, but hamper internal communications. (Doctrine)
- Operational activity is limited by intelligence, as well as a requirement to influence public perception. (Operational Methods/Information Strategy)
- The inter-connected aspects of network structure provide a vulnerability to infiltration. (Organization)

[247] U.S. Department of Defense, Joint Publication 3-26, *Counterterrorism*, III–15.

It is clear that networks have vulnerabilities, and these vulnerabilities provide the starting point for the formulation of basic hypotheses for countering networks. These hypotheses are further developed using insights from irregular warfare theories and approaches, primarily counter-insurgency and counter-terrorism. Key variables from these hypotheses are then examined using four major models, representing primary approaches to countering irregular opponents. In addition, it is clear that contextual and environmental factors must also be considered. For instance, what is the primary strategy pursued by these rogue networks? Is it a popular insurgency, or is the network being challenged more of a clandestine terrorist network with few ties to the larger population? Fighting networks are elements of a larger social network structure, and understanding the population they interact with may be as critical to their disruption, as any other insight. Fighting networks are not standard military opponents, and in many cases, the primary effort must be "persuading the population."[248] The complexities of were, how, and why people interact are essential aspects of understanding the different nature of collecting intelligence in an irregular warfare environment. Cultural factors are obviously important as well, and they will influence the specific nature of these vulnerabilities. These vulnerabilities and the hypotheses that follow must be placed in light of unique cultural factors and strategic considerations. As Kilcullen states about COIN, "instead of approaching the threats we face solely on the plane of tactical or operational questions and making the choice of which field manual we should use in theater a primary issue—rather than treating this properly as a doctrinal issue—we should start by establishing the context of the conflict."[249] Gordon Hahn reinforces this by stating, "efforts to split the insurgency cannot succeed without a detailed understanding of the network's political, social, tribal, and economic cleavages. Detailed knowledge of the insurgent network's historical, cultural, political-ideological, and structural intricacies is also essential."[250]

---

[248] Michael T. Flynn, Matt Pottinger, and Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan* (Washington, DC: Center for a New American Security, 2010), 24, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA511613&Location=U2&doc=GetTRDoc.pdf.

[249] Sebastian L. V. Gorka and David Kilcullen, "An Actor-Centric Theory of War: Understanding the Difference between COIN and Counterinsurgency," *Joint Forces Quarterly* 60, no. 1 (2011): 18, National Defense University Press, http://www.ndupress.ndu.edu.

[250] Hahn, "The Jihadi Insurgency and the Russian Counterinsurgency in the North Caucasus," 3.

With those imperative notes of caution in mind, and recognizing the critical importance of strategic decision making, the following hypotheses serve as a guideline to counter fighting networks.

3. Counter Network Hypotheses

- The decentralized nature of networks may be countered by similar units taking the offensive against them.

Fighting networks tend to favor the offensive form of maneuver, even though they blend, and often blur, aspects of offense and defense. In this regard, networks seek to attack when they have the initiative and when conditions provide for relative combat power at the point of attack. Further, networks must maintain an element of surprise to be offensively effective. Nodes are generally smaller to ensure that they maintain concealment up to the point of attack, thereby gaining surprise. A recent example of such decentralized small unit action is seen in the number of Taliban attacks against security installations in Afghanistan. These attacks are conducted by small, usually no more than 4–6 attackers, cells that have increasingly used their opposition's uniforms to conceal their infiltration and attacks against much stronger and heavily fortified targets.[251]

These aspects of the offense may be mitigated, and even countered by a similarly offensive approach. This approach is especially effective if conducted at the tactical level against the distributed nodes that form a network. In essence, by taking the offensive against these nodes, they are unable to strike using their initiative. Faced with pressure from attacking nodes able to deny their use of surprise, nodes within a fighting network find themselves in a position where they are either forced to evade, defend at the tactical level, or band with other nodes to mount a concerted counterattack. Nodes that are evading are at the mercy of their opponent's ability to maintain contact, or track them. Nodes that attempt to defend in isolation are quickly overwhelmed. Nodes able to work

[251] Bilal Sarwary, "Shift in Taliban Tactics Alarms Afghanistan Government," May 29, 2011, *BBC News South Asia*, http://www.bbc.co.uk/news/world-south-asia-13589764.

in concert may achieve success with a counter-swarm, but will require excellent communications, enough agility to reinforce disparate nodes, and synchronized C2 to regain the initiative.

- Network synchronization requires an overarching purpose, which may be negated by a focused information strategy.

This fact is noteworthy because networks require synchronization to be effective, and without an overarching purpose, it is difficult to conduct coordinated swarming among autonomous nodes. For networks to achieve significant success, they must find ways to synchronize dispersed nodes with high degrees of autonomy.[252] The purpose provides an overall cohesive function that is powerful, and serves as an adhesive that permeates every aspect of the network.[253] The al-Qaeda network shows how a consistent vision and set of ideas may be used to expand influence and generate a significant, even global, cohesive effect.[254] However, if this purpose becomes less attractive, or if the motivating cause loses its luster, the adhesive effect that it provides may not withstand the pressures of conflict.

A purposeful and directed information strategy, aimed at countering a network's purpose and goals, may have significant effect in disrupting a network's ability to operate with unity of effort. Anthony Pratkanis describes the use of social influence as a primary element to counter an enemy's purpose, by changing minds and behavior within the network, "social influence uses tactics that appeal to our human nature to secure compliance, obedience, assistance, and behavior and attitude change."[255] Moreover, Pratkanis notes, "in a social influence campaign, just as in physical warfare, the influence strategy of adversaries and competitors must be attacked."[256] The initial aspect of this influence strategy is the network's purpose, or cohesive vision, and it will be the most

---

[252] Eilstrup-Sangiovanni and Jones, "Assessing the Dangers of Illicit Networks," 22.

[253] Ronfeldt, "Al-Qaeda and its Affiliates," 43.

[254] al-Suri, "The Global Islamic Resistance Call," 347–484.

[255] Anthony R. Pratkanis, "Winning Hearts and Minds: A Social Influence Analysis," in *Information Strategy and Warfare: A Guide to Theory and Practice*, ed. John Arquilla and Douglas A. Borer, 56–80, (New York: Routledge, 2007), 57.

[256] Pratkanis, "Winning Hearts and Minds: A Social Influence Analysis," 58.

important aspect of countering networks over time. Unfortunately, its importance rarely receives a commensurate level of action, for instance, "of all the U.S. government's actions since 9/11 to counter the threat of global militant Islamism, its weakest response by far has been its strategic communications and public diplomacy efforts."[257] Correctly assessing a network's environment and information strategy remains fundamental, and disruption efforts should be prioritized against those findings. Interestingly, one of the most effective ways to counter a rogue network's purpose may be to simply expose and publicize its violent actions.

- The extensive communication that characterizes networks may be countered by denial and collection activities.

Communication is essential to synchronizing and utilizing the network form, and networks require considerable communication between nodes and clusters of nodes. The flattening of information technology and its global access provides capability for networks, but also vulnerabilities to disruption activities.[258] While the ability to communicate rapidly throughout the network is a strong feature of networks, it also creates additional requirements for unified action. Networks thrive on constant communication, but the pressures they face in conflict, and the requirements for secrecy, work against large volumes of open communication. In this way, fighting networks are constrained, and where they do use open forms of communication, such as the Internet and telephones, they face extensive risk of compromise.

Concerted effort against a network's communications, to include person-to-person verbal, telephonic, internet, courier notes, and even simple signals, is an imperative to countering a network's communication attributes. These counter-efforts have two basic forms, denial and collection, and both serve to disrupt a network's communications, and ultimately, their flow of information. In addition, in many cases, networks use the same linkages between nodes to pass resources (economic or material), which adds to the value

[257] CAPT Timothy J. Doorey, "Waging an Effective Strategic Communications Campaign in the War on Terror," in *Ideas As Weapons: Influence and Perception in Modern Warfare*, ed. G. J. David Jr. and T. R. McKeldin II (Washington, DC: Potomac Books, 2009), 145.

[258] Calvert W. Jones, "Exploiting Structural Weaknesses in Terrorist Networks: Information Blitzkrieg and Related Strategies," in *Ideas as Weapons: Influence and Perception in Modern Warfare*, ed. G. J. David Jr. and T. R. McKeldin, III (Dulles, VA: Potomac Books, Inc., 2009), 7.

of disrupting communications. Of the two forms, denial is best characterized as denying the opponent the ability to transmit between nodes, or collectively through the network as a whole, by severing or blocking, the use of linkages. This denial may be accomplished in numerous ways and through multiple mediums; for example, in cyberspace, the use of degradation through "blitzkrieg" techniques on message boards, phishing scams, and other activities results in a polluted and less effective communications environment.[259] This results in less overall communications between nodes and a dramatic decrease in network efficiency. The trade-off with denial activities is that reduced communications levels provides less overall signature for illumination, and so they must be undertaken in a pulsing manner, or when further collection is not required. The other form, collection, focuses on allowing full use of all the linkages in a network, and rather than deny them, it gains access to the information or resources flowing across the linkages. This collection effort provides the conduit for deception campaigns, or gaining tremendous insight on the network's structure and plans to allow for decisive pulsing attacks. Both aspects, used in conjunction and weighted according to priorities, provide the basis for disrupting a networks information flow.

- Network concealment may be diminished by illumination activities.

The basic force asymmetry in irregular conflict requires networks to maintain their concealment. Without concealment, the dispersed nodes within a network are increasingly vulnerable, and they obtain this concealment through being able to "hide" within population groups, as well as utilize restrictive terrain. Without this concealment, the small, dispersed nodes that create a network are vulnerable to rapid identification and removal from the network. Intelligence on networked opponents requires maintaining close contact with the constantly changing network. The degree to which the network is homogenous (physically and ideologically) with the population provides a significant indicator of the amount of concealment it will enjoy. Networks that may not be able to hide fully within the population will require the use of terrain to gain separation and

[259] Jones, "Exploiting Structural Weaknesses in Terrorist Networks," 10.

camouflage. Cyberspace, in addition to providing communicative and instrumental uses, also serves a form of terrain, providing concealment in the form of the anonymity and freedom of maneuver that it grants nodes within a network.[260]

Illumination efforts address the concealment requirement of fighting networks and provide a way to expose both their structure and activities. These efforts recognize that intelligence activities are paramount in countering networks, and constitute the essence of the "hider-finder" dynamic that defines much of irregular warfare.[261] However, illumination efforts go beyond traditional characterizations of intelligence, and must infuse every counter-network activity and take on an operational nature that is very different from passive analysis. As Gregory Treverton states, "the change [in targets] is widely acknowledged, yet its implications run far deeper than are usually recognized. The change goes to the heart of how intelligence does business—from collection to analysis to dissemination, to use labels that are increasingly less apt."[262] The nature of the concealment largely determines the methods and scope of employment to strip away concealment and locate elements within the network, as well as develop a larger picture of how the network operates. Multiple tools and efforts must be employed, and a baseline understanding of the social networking ties is crucial to mapping out larger portions of the network, and guides infiltration and disruption efforts. Incorporating some of the most visible aspects of network activity, operational actions provide details because networks reveal themselves. Operational activity is nearly always visible (it is the most unique as visible aspect of clandestine networks) to some degree; fighting networks must fight to remain relevant.[263] The overt activity they conduct provides strong leads towards identifying the actors conducting such activity. In addition, continued pursuit using exploitation activities furthers illumination activities, revealing more about the network through close, persistent contact.

---

[260] Weimann, *Terror on the Internet*, 67.

[261] Arquilla, "The End of War as We Knew It?," 389.

[262] Treverton, *Intelligence for an Age of Terror*, 15.

[263] Ibid., 41–48.

- Network structures are vulnerable to specific damage against their hubs, which is achieved through precise and high levels of active targeting.

The very nature of network structures provide for a great deal of resiliency, as well as an impressive ability to grow through preferential attachment. Preferential attachment is a common characteristic of social networks, which primarily exhibit a free-scale nature.[264] Fighting networks are free scale and grow by nodes attaching themselves to other nodes based on a variety of factors, not through random placement, and the increasingly connected nodes become hubs. These hubs serve a critical function, as "it is the highly connected hubs that account for the difference between the two networks, as the hubs act as a kind of glue within the network. Since an uncoordinated attack targets elements at random, it almost always knocks out unimportant elements with few links, while missing the hubs."[265] While the nature of free-scale networks make them somewhat resilient in the face of random attacks, it appears possible that a concerted effort against the highly-connected hubs could lead to dramatic effects. As the ground-breaking research by Barabási and others describes, this is a classic vulnerability of free-scale network structure.[266] Other research supports this vulnerability, and shows that while targeting a leader in a hierarchy has a significant effect, "it may be necessary to simultaneously remove more nodes to have the same impact on a distributed decentralized system."[267]

In countering free-scale networks, the primary goal is to neutralize hubs at a rate faster than which they are able to form. These hubs hold significant expertise, communicate extensively, provide direction, and establish cohesion. Sageman discusses targeting these hubs as part of a concerted effort to counter terror networks, stating that the presence of hubs means that terrorist networks, "…are particularly vulnerable because most communications and human contacts go through them. Arresting these individuals

---

[264] August Hammerli, Regula Gattiker, and Reto Weyermann, "Conflict and Cooperation in an Actor's Network of Chechnya Based on Event Data," *Journal of Conflict Resolution* 50, no. 2 (April 2006): 172, http://www.jstor.org/stable/276638482.

[265] Buchanan, *Nexus*, 132.

[266] Barabási and Albert, "Emergence of Scaling in Random Networks, 509–512; Barabási and Bonabeau, "Scale-Free Networks," 60–69.

[267] Carley, Lee, and Krackhardt, "Destabilizing Networks," 88.

would degrade these networks into isolated units, singletons, or cliques, who would consequently be incapable of mounting complex large-scale operations…"[268] According to Treverton, "moreover, the transnational arena involves networked actors subject to what students of the emerging science of networks refer to as 'cascades,' making them more vulnerable to sudden change than state-to-state systems….small changes within the network accumulate until the network reaches a 'tipping point,' after which a dramatic domino-like sequence ensues…"[269] This approach requires a high level of operational activity, and activity that must be closely tied to an understanding of the network itself, which renders the problem of destabilization more difficult for a network than for a hierarchy.[270]

- Networks are isolated without an effective means to influence public opinion, which may be denied through a combination of information disruption and operational pressure.

Networks in the information age grasp the importance of influencing public opinion, but this also serves as a limiting function for the type and nature of the operations they conduct. The irregular warfare networks that require a significant degree of influence among the population, such a popular-based insurgent network, must conduct operations consistent with their overall narrative. This limits the activities available to these fighting networks, making them reliant on persuading the population at a local level. This is evident in amount of time and resources such networks devote to these efforts.[271] Terror networks employ more of a coercive effect, and use the population as a means of transmitting their message through terror tactics. If networks are unable to achieve either a persuasive effect, or a coercive effect on their target audience, then their operational activity falls short of achieving a larger strategic effect. In fact, this operational activity might actually backfire and result in violent action with no meaning.

---

[268] Sageman, *Understanding Terror Networks*, 176.

[269] Treverton, *Intelligence in an Age of Terror*, 31.

[270] Carley, Lee, and Krackhardt, "Destabilizing Networks," 88.

[271] Rid and Hecker, *War 2.0*, 129.

Denying networks the means to influence public opinion is a challenging task, given the ubiquitous nature of information technology and access to social media. However, denial may be more a form of limiting the nature of the message relayed, rather than actually blocking the form of messaging itself. By increasing pressures on the network, reducing flexibility in messaging, and proactively determining the nature of the information struggle, counter-network efforts may be able to channel the actual information content that a network produces. The difficulty of this effort increases with the ease of access and openness of information services available to fighting network, but it may be the most decisive aspect of countering such networks. Such efforts require more than just physical strikes against media broadcasting towers, and require a concerted effort against physical technologies, communicating nodes, and audiences. Operational pressure complements such focused activity, but reduces options to communicate through imposing increased costs. Preventing an information asymmetry in the network's favor is an essential step to reducing their greatest strength in irregular conflict.

- All-channel connections and aspects of larger network formation allow infiltration into the network.

As networks are largely self-generating, open systems, few controlling mechanism governing their formation exist. Weak ties provide the mechanism for larger network formation by linking clusters of well-connected nodes into other clusters, and by doing, so providing a bridging mechanism. While the ability to grow by expanding freely and generating connections to new nodes is a positive feature of network organization, these advantage also create vulnerabilities. The network form facilitates recruitment, due to its dispersed and tailored local nodes.[272] This recruitment is largely driven by social connections from the bottom-up, rather than any formal to-down vetting.[273] In addition, the use of the Internet for recruitment provides another avenue for infiltration. Since the Internet carries with it a degree of autonomy, it provides a potential access point for initial contact with networks. While the proliferation of jihadist website increases the

[272] Eilstrup-Sangiovanni and Jones, "Assessing the Dangers of Illicit Networks," 14.

[273] Sageman, *Understanding Terror Networks*, 169.

reach of terror networks, and favors recruiting, the fact that "signing up for the jihad was just a click of a mouse away," provides increasing opportunities for infiltration as well.[274]

It is easier to infiltrate networks than other types of organizations with formal, hierarchically controlled vetting. Although strong ties exist within networks, the weak ties that lead to increased scaling provide opportunities for accessing the network. A group of infiltrators would find it relatively simply to "bond" within a network by utilizing the weak ties that serve as brokers. In this regard, the use of pseudo-ops is instructive. These operations, as conducted by counter-insurgents, replicate guerrilla units, which then infiltrate and locate actual guerrilla organizations. Overall, they have had mixed results, but several effective examples shows potential for their use given the appropriate conditions.[275] In addition, cyberspace provides a high degree of anonymity, which increases the possibility of contact with network brokers and facilitates the ease of joining a network.

4. Variables Associated with Effective Counter-Network Operations

Each of the preceding propositions leads to the development of variables, which contribute to countering networks. These variables have multiple aspects, and their interaction contributes to the overall development of effective counter-network operations. These variables do not stand alone, but are essential and mutually reinforcing. The first three variables demonstrate actions taken to counter networks, while the last, fusion, describes features, which provides the fundamental capability to undertake effective counter-network action.

---

[274] Peter Bergen, *The Longest War: The Enduring Conflict Between America and Al-Qaeda* (New York: Free Press, 2011), 213.

[275] Perhaps the most notable modern work on the subject of pseudo-operations is MAJ Frank Kitson's work on their usage in the British response to the Kenyan Mau-Mau insurgency, see MAJ Frank Kitson, *Gangs and Counter-Gangs* (London: Barrie and Rockliff, 1960); another fascinating account is the LTC Ronald Reid-Daly's account of similar operations during the Rhodesian conflict, see, LTC Ronald F. Reid-Daly, *Pamwe Chete: The Legend of the Selous Scouts* (Weltevreden Park, South Africa: Covos-Day, 2000); a brief compilation of other usages is found in Lawrence E. Cline, *Pseudo Operations and Counterinsurgency Lessons from Other Countries*, United States Army War College Strategic Studies Institute, June 2005, http://www.carlisle.army.mil/pubs/display.cfm?pubID=607.

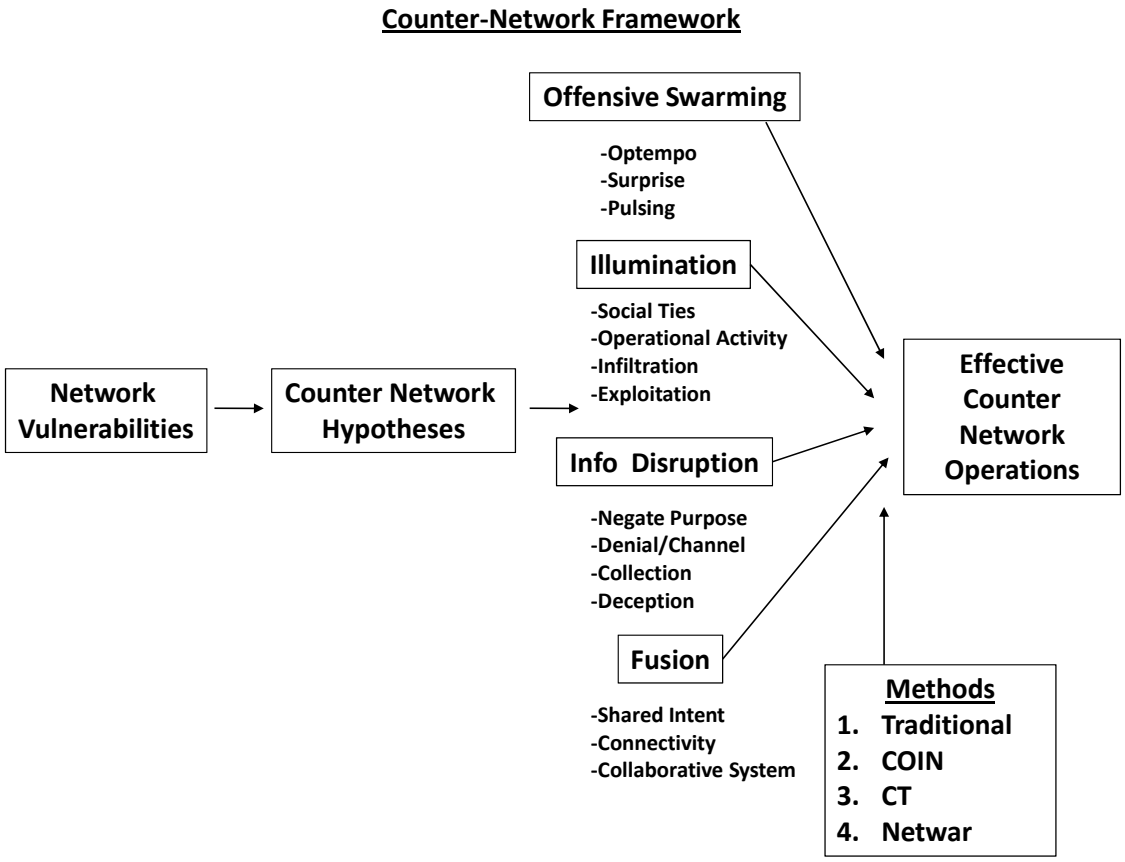

Figure 9. A Framework for Developing Counter-Network Theory

a. Illumination

The first variable is illumination, which describes the counter-network efforts that address a network's concealment vulnerabilities. Illumination goes beyond traditional intelligence and is based on the nature of how networks fight. It provides the means to identify and locate the dispersed nodes within a fighting network. There are four primary methods to "illuminate" the dark aspects of fighting networks. Each of these ways addresses unique aspects of the network, but they are most effective when used in a combined manner. In fact, their fusion produces an overall effort that is far more effective than any singular focus.

The first method utilizes social ties, or the popular base of support and the social networks from which the fighting network formed. The strong social networks that provide strength for networks create opportunities for illumination with the right perspective. The primary reason that these social structures provide a means of illumination is because networks make extensive usage of the strong ties within the social structure. Strong ties are a significant aspect of network formation, but the social linkages that form these ties exist in an open, "unsecure manner." Ironically, much intelligence collection focuses directly on the irregular opponent, not realizing the vast amount of information available that could aid in illumination efforts. In an article calling for a restructuring of intelligence collection efforts in Afghanistan, General Michael Flynn highlighted the importance of "gaining and exploiting knowledge about the localized contexts of operation and the distinctions between the Taliban and the rest of the Afghanistan population."[276] This knowledge is critical to understanding the ties between fighting network combatants and the local population. As previously discussed, the high-risk nature of irregular clandestine conflict develops strong ties, which are characterized by high degrees of trust. These trust-based relationships are primarily based on friendship and kinship ties.[277] These dense networks of relationships provide a significant means to identify core network segments, despite their efforts to remain hidden. In addition, it may be possible to erode trust and create further destabilization within the network.

Another illumination method is to force the network to display itself operationally. In essence, this method forces the network into launching operational attacks, which makes operational nodes highly visible, and hence, subject to targeting. This operational aspect is a function of the pressure exerted against a network that forces networks to either hide or evade. Both of these actions require clandestine mechanisms, but the more clandestine a network is, the more inefficient it is. A highly clandestine network resorts to a more structured cellular form, and requires more authority to enforce. In seeking to maintain these clandestine aspects, ensuring cut-outs, limiting communication and travel, etc., a network reduces connections, slows communication,

[276] Flynn, Pottinger, and Batchelor, *Fixing Intel*, 23.

[277] Sageman, *Understanding Terror Networks*, 178.

and loses many of the all-channel aspects that made it so operationally effective. Thus, this operational aspect and the pressure that it brings presents a fundamental choice for fighting networks—either maintain operational activity, and face increased pressure, or scale back operational activity and seek to become more clandestine, but in the process, become increasingly structured and insular. This balancing activity that a network must maintain is a function that may be exploited by those seeking to counter fighting networks. By forcing a network to make these difficult choices, they are "putting the enemy on the horns of a dilemma."[278]

The third method is the exploitation of the network itself, or using existing connections to turn it "inside-out." Exploitation consists of interrogation, but also includes information on the network from a variety of sources, including technical means and traditional human intelligence (HUMINT). The primary elements of HUMINT in this environment are classic espionage and detainee interrogations.[279] Traditional methods of countering dispersed and elusive irregular networks focus on the necessity for interrogation as a critical part of a larger intelligence gathering enterprise. While some counter-insurgents argued for the necessity of interrogations to justify torture,[280] the British Special Police under Sir Gerald Templar provided examples of interrogations conducted in a manner that provided both information, preserved dignity, and expanded illumination opportunities.[281] Modern COIN doctrine continues to stress the importance of interrogation, and its role in understanding the nature of the threats in an irregular environment.[282] Detainee interviews or interrogations may provide an exceptional level

[278] William Tecumseh Sherman utilized this phrase in his memoirs to describe forcing an enemy into a difficult strategic choice, and is cited in B.H. Liddell Hart, *Strategy*, 343.

[279] Human Intelligence (HUMINT) has classically referred to espionage and is primarily focused on the principal-agent relationship. However, the U.S. Department of Defense doctrinally describes HUMINT as consisting of both source-driven intelligence, as well as detainee interviews and interrogations. (Joint Publication 2-0, *Joint Intelligence*, I–6). This broader definition is more appropriate to irregular warfare, and aids in efforts to establish an effective fusion of intelligence methods and operations.

[280] Roger Trinquier, *Modern Warfare: A French View of Counterinsurgency*, trans. Daniel Lee (Westport, CT: Praeger Security International, 2006), 19.

[281] Bruce Hoffman and Jennifer M. Taw, *Defense Policy and Low-Intensity Conflict: The Development of Britain's 'Small Wars' Doctrine During the 1950s* (Santa Monica, CA: RAND, 164), 27–29.

[282] U.S. Department of Defense, Field Manual 3-24, *Counterinsurgency*, 3–27.

of information because their subjects are actually within the enemy network. Modern counter-network efforts reinforce this timeless lesson, simply stated by noted counter-insurgent theorist Julian Paget, "…patrols, observation and, above all, prisoners who can be interrogated are of the greatest value."[283] In fact, it may provide the only means "…to reach deeply into small groups—their proclivities and capabilities—to provide an understanding that can lead to preventive action."[284] A current example of this level of understanding is the capture and subsequent information gained from the German citizen Ahmed Sidiqi, which prevented a major series of terror attacks in Europe.[285] In addition, detainee interrogation is conducted with the aid of law-enforcement-derived techniques to ensure that evidence is recovered, and used as leverage.

The all-channel nature and use of weak ties to connect varies network segments provide for increased avenues for infiltration. While a high degree of connectivity is an advantage that allows for rapid information flow, it also allows for increased access to information and more contact than in other organizational forms. In addition, the weak ties that serve as bridges within a network mean that the initial access into a network is rarely closely scrutinized, or vetted. Ties formed for recruitment, support activities, and even friendship, provide avenues to access and begin revealing network activities. The case of the noted terrorist Razmzi Yousef, connected to al-Qaeda plots and betrayed by a friend he met at the Islamic University in Islamabad years earlier, is a notable example.[286] Another notable example, which demonstrates the same effect on the Internet, is the Montana mom, Shannon Rossmiller, who uses online social networking sites to befriend, and then betray, jihadists; maintaining profiles on over 600-suspected individuals.[287] In addition to these examples of HUMINT penetration, the use

---

[283] Paget, *Counter-Insurgency Operations*," 163.

[284] Treverton, *Intelligence for an Age of Terror*, 2.

[285] Michael B. Mukasey, "How a Bagram Detainee Foiled the Euro Terror Plot," *Wall Street Journal*, October 8, 2010, 19. Even more recently, early reports about the death of Osama Bin Laden describe how interrogation provided the initial leads instrumental in identifying the support network that enabled his efforts.

[286] Jones, "Exploiting Structural Weaknesses in Terrorist Networks: Information Blitzkrieg and Related Strategies," 11.

[287] Noah Shachtman, "Some of Her Best Friends Are Terrorists," *WIRED*, October 23, 2007, http://www.wired.com/dangerroom/2007/10/some-of-her-bes/.

of pseudo-operations may prove to be of value as well. In fact, in dispersed networks and throughout a larger homogenous population, great potential for decoy activities and false groups exists.

b. Offensive Swarming

Swarming provides the most valid counter to the distributed nature of fighting networks. These networks are composed of dispersed nodes that even when converged upon are difficult to target due to their use of standoff and evasion. However, counter-nodes that have the same agility and speed may counter these nodes. The decisive aspect of the counter-nodes would be a greater empowerment at the local level, most likely gained through a combination of nodes and technologies, as well as increased situational awareness gained through superior connectivity throughout.

These counter-swarming units would fight on the offensive, and deny the enemy its required surprise by continually forcing it either to hide or evade. Fighting networks generally require surprise to be operationally effective. While the nature of surprise is not necessarily a zero-sum equation between two opponents, it is largely exercised by the side gaining the initiative. This initiative is possible because the opponent is caught off-guard. As William McRaven noted, when describing the offensive nature of small special operations units, surprise is a factor of deception, timing, and taking advantage of an opponent's vulnerabilities.[288] Swarming provides a combined method for those countering networks to achieve surprise consistently, and generate the operational pressure that denies it to opponents.

A key aspect of offensive swarming is pulsing. Pulsing is a function of watching and waiting balanced with rapid strikes against vulnerabilities, followed by redispersal of nodes into a collection posture. Initial descriptions of pulsing describe it as a fundamental aspect of swarming, "swarming is seemingly amorphous, but it is a deliberately structured, coordinated, strategic way to strike from all directions, by means of a sustainable pulsing of force and/or fire, close-in as well as from stand-off

[288] William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice* (Novato, CA: Presidio Press, 1995), 17.

positions."[289] As a swarming characteristic, pulsing incorporates intelligence gained through illumination to determine the tempo and nature of strikes against a network. The initiation and re-initiation of sustained pulsing differentiates it from guerrilla tactics.[290] The periods between attacks may be relatively short, but they allow for the identification of new vulnerabilities and the synchronization of this intelligence.

In addition, offensive swarming of this nature would be characterized by a high level of operational tempo, or "optempo" designed to destroy hubs rapidly, forcing an unsustainable replacement rate. Free-scale networks cannot sustain a high rate of loss, especially from those operationally active elements, the hubs that provide such a cohesive and critical element of its structure. While it is a generally accepted notion that losses in networks are easily filled by replacements, this may not necessarily be the case. In instances where losses are replaced, it is questionable whether they are replaced with the same level of expertise, and whether actors with the same level of operational importance and connectivity fill hub positions. Further, blind attrition may actually "sharpen" a network by providing the opportunities for more motivated replacements stepping up, replacements trained by current experience. To mitigate such effects, significant operational activity must be focused with extensive illumination efforts, which ensures that the overall damage created within a network's structure is greater than the replacement value of individual nodes.

c. Information Disruption

Information disruption counters a network's reliance on information, and seeks to exploit the weaknesses revealed in a network's information strategy. As Berkowitz indicates, the most important factor defining military power in the information age is the "….ability to collect, communicate, process, and protect information," and that winning the information war requires, "…making your own information systems more capable, reliable, and secure, or by attacking your opponent's systems so that they are

[289] John Arquilla and David Ronfeldt, *Swarming and the Future of Conflict* (Santa Monica, CA: RAND, MR-1100-OSD, 2000), vii.

[290] Edwards, *Swarming and the Future of Warfare*, 68.

less capable, less reliable, and less secure."[291] According to Lawrence Freedman, "in irregular warfare, superiority in the physical environment is of little value unless it can be translated into an advantage in the information environment."[292] Kilcullen reinforces this imperative as well, stating that, "it's now fundamentally an information fight, the enemy gets that, and we don't yet," when insurgent networks attack a vehicle in Iraq, for instance, "they're not doing that be because they want to reduce the number of Humvees we have in Iraq by one. They're doing it because they want spectacular media footage of a burning Humvee."[293] These dynamics make a proper information strategy an imperative, and require that efforts to counter networks have a robust information disruption component. This component is not a stand-alone element, but must be tightly synchronized with operational efforts, fused within a larger illumination effort.

The primary aspect of this variable is a focus on negating the networked opponent's overall purpose and goals. A strong cohesive element in network formation is a shared outlook, or narrative, that unites dispersed and relatively autonomous nodes. This narrative is a driving factor in how the network behaves and provides the motivating cause for much of a network's actions. Information disruption seeks to counter this overarching purpose through weakening, distorting, and perhaps even ignoring a fighting network's stated purpose.

The second aspect of information disruption is focused on denying, or channeling, a network's ability to communicate. This effort seeks to reduce the amount of information flow within both the network and external communications outside the network. Efforts to reduce internal information flows focus on isolating actors that would otherwise serve as communication hubs, as well as sowing distrust to slow and even

[291] Berkowitz, *The New Face of War*, 21.

[292] Lawrence Freedman, *The Transformation of Strategic Affairs* (Abingdon, NY: Routledge, 2006).

[293] George Packer, "Knowing the Enemy: Can Social Scientists Redefine the 'War on Terror?'" *The New Yorker*, December 18, 2006, 65–66, http://www.newyorker.com/archive/2006/12/18/061218fa_fact2.

block information that would otherwise be shared. These efforts, in addition, to the normal costs incurred by the clandestine nature of fighting networks, provide critical disruptive effects.[294]

The third aspect of information disruption is to allow the network to communicate as much as possible, and use the information provided to further understand and illuminate the network. This technique is increasingly viable in an age in which verbal intelligence, primarily in the form of SIGINT, but also in cyberspace, provides considerable information.[295] This technique requires considerable balance between operational activity and the ability to gain additional information on the network.

Woven throughout the conduct of information disruption is the ability to achieve deceptive effects as well. Deception provides strategic options while facilitating economy of force, and it may serve as a critical tool in countering a network's aims. If a cloak of deception over the whole enterprise of irregular warfare exists, it may be that various deception stratagems may prove effective in disrupting both internal and external information flows.[296]

d. Fusion

Fusion is a counter to the synchronized connections employed by networked opponents, and has both an organizational element, and a doctrinal element. Organizationally, fusion requires a high level of network-like connectivity between elements, and is essential for collaborative efforts.[297] Doctrinally fusion involves the incorporation of a range of operational capabilities and analytic efforts in a systematic problem-solving process. It empowers both intelligence and operations by "fusing" them

---

[294] Bell, "Aspects of the Dragonworld," 27–31.

[295] Kahn, "A Historical Theory of Intelligence," in *Intelligence Theory*, 10.

[296] Latimer, *Deception in War*, 272.

[297] Organizationally, fusion provides a structural framework that maximizes cultural intelligence and collaboration by effectively combining diverse actors or groups in ways that encourages information sharing and decision-making. See, for example, Michael Heffner and Nawaz Sharif, "Knowledge Fusion for Technological Innovation in Organizations," *Journal of Knowledge Management* 12, no. 2 (2008): 79–93; Maddy Janssens and Jeanne M. Brett, "Cultural Intelligence in Global Teams: A Fusion Model of Collaboration," *Group & Organizational Management* 31, no. l (February 1, 2006): 124–153.

in a manner that both acquires tremendous intelligence and produces disruptive operational effect against irregular opponents. While preliminary analysis of intelligence "fusion cells" notes their effectiveness in combining multiple aspects of intelligence to produce a common picture, the fusion described here goes beyond just intelligence sharing.[298] Intelligence fusion cells are a necessary component for producing greater connectivity, but they are not nearly sufficient if not complement and tightly connected to operational efforts.

In the irregular conflict environment, intelligence plays a primary role, and even operations must be designed to generate intelligence. According to Frank Kitson, "if it is accepted that the problem of defeating the enemy consists very largely of finding him, it is easy to recognize the paramount importance of good information."[299] Irregular warfare history shows that an inability to recognize the nature of the irregular warfare environment leads to a failed reliance on simple operational activity to find the enemy. For example, during the U.S. Marines counter-guerrilla patrolling efforts in Nicaragua over a five-year period from 1927–1932, only one patrol in 20 managed to make contact with guerrilla forces.[300] Operations and intelligence fusion provides a level of connectivity that facilitates synchronization of effort and the sharing of information required to achieve success in each of the previous variables. While the previous three variables are focused on actions taken specifically against networks, fusion focuses on a core capability required to conduct such actions.

Shared intent provides an overall direction for the counter-network effort, and this purpose is critical for any organization, especially one that provides a greater

---

[298] See, for example, David L. Carter, "The Intelligence Fusion Process," *Intelligence*, 2008; LCDR Christopher L. Fussell, MAJ Trevor M. Hugh, and MAJ Matthew D. Pedersen, *What Makes Fusion Cells Effective?* (Master's thesis, Monterey, CA: Naval Postgraduate School, 2009); David L. Carter and Jeremy G. Carter, "The Intelligence Fusion Process for State, Local, and Tribal Law Enforcement," *Criminal Justice and Behavior* 36, no. 12 (2009); Kevin D. Eack, "State and Local Fusion Centers: Emerging Trends and Issues," *Homeland Security Affairs*, http://www.hsaj.org/index.php?fullarticle=supplement.2.3.

[299] Frank Kitson, *Low-Intensity Operations: Subversion, Insurgency, Peacekeeping* (London: Faber & Faber, 1971), 95.

[300] Michael J. Schroeder, "Intelligence Capacities of the U.S. Military in the Sandino Rebellion, Las Segovias, Nicaragua, 1927–1932: Successes, Failures, Lessons," 3, http://sandinorebellion.com/mjs/mjs-intel.htm.

deal of autonomy.[301] Fusion requires a shared intent to bring together disparate elements and provide an overarching purpose that translates into specific goals. This intent unites disparate organizational goals and focuses in ways that maximizes contributions to specific tasks. Despite fusion producing an "inversion of expertise," through greater connectivity and innovation at the lowest levels, leadership is crucial in providing and emphasizing a shared intent.[302]

Comprehensive connectivity between people, information, and effort provides the synergy required to facilitate actions like illumination and swarming. The connectivity within an organization is a result of its general configuration, and changes in configuration may increase effectiveness by an order of magnitude.[303] While most organizations establish connections between people, information flows and efforts are channelized and structured to produce efficient task production. Organizations have properties and functions that are larger than the actors within them are. In fact, these properties are characteristics of the whole, and are often beyond the scope and comprehension of individual actors, but largely determine an organization's effectiveness.[304]

The irregular warfare environment requires a system that facilitates fusion. Both the pace and disruptive effect of operations places challenging demands on intelligence, as friendly operations and the enemy's adaptive response continuously change the enemy's location and structure. Given this dynamic, operations both require and yield intelligence, creating a cycle with the ultimate purpose of gaining a greater understanding about the enemy. A notable historic example is the British experience in Malaya, where the Special Branch Police provided an over-arching intelligence collection

---

[301] Jon Katzenbach and Douglas Smith, *The Wisdom of Teams: Creating the High Performance Organization* (Boston: Harvard Business School Press, 1993), 21.

[302] Stanley McChrystal, "Listen, Learn, … then Lead," remarks presented at the TED Conference, March 2011, http://www.ted.com/talks/stanley_mcchrystal.html.

[303] Nicholas A. Christakis and James H. Fowler, *Connected* (New York: Little Brown and Company, 2011), 8.

[304] Ibid., 25.

focus, and operational units worked to support these efforts.[305] The fundamental evolution in modern irregular warfare addresses the illumination challenge by providing a decentralized system at the operational level. The focus of this system supports and generates intelligence at the lowest levels, rather than simply pushing intelligence higher. In essence, a fusion of intelligence capacity with operational efforts provides a new level of synergy at the lowest levels, generating un-paralleled agility. While intelligence collection is still the over-arching focus, intelligence and operational efforts are decentralized, and often co-located through dramatic advances in information technology. This is a system where both the collector and the consumers achieve high levels of collaborative work since a targeting cycle provides a common focus.[306] Intelligence collection is the primary focus of operational activity and collected intelligence supports further operations. Further, the focus of operational support and advances in information technology provide means to ensure that the targeting cycle is as robust as possible. A powerful recent example is the dramatic function of airborne Intelligence, Surveillance, and Reconnaissance (ISR) within the targeting cycle. "Airborne ISR has become critical in this war because it offers persistent and low-visibility observation of the enemy as well as an ability to detect, identify, and track him in this low-contrast [urban or rural] environment."[307] ISR provides a unique capability that allows for the fusion of all-source intelligence and operational input, and is a primary element in the modern targeting cycle.

---

[305] Riley Sunderland, *Antiguerrilla Intelligence in Malaya, 1948–1960* (Santa Monica, CA: RAND Corporation, 1964), vii.

[306] The targeting cycle has multiple elements, but the most successful modern form is the F3EAD model. This model of Find, Fix, Finish, Exploit, Analyze, and Disseminate describes a cyclical relationship of both operational and intelligence related activities designed to generate a comprehensive understanding of the entire network. See, for example, Christopher J. Lamb and Evan Musing, "Secret Weapon: High-Value Target Teams as an Organizational Innovation," *Institute for National Strategic Studies Strategic Perspectives*, no. 4 (2011): 33, and LTC William J. Hartman, "Exploitation Tactics: A Doctrine for the 21st Century," Monograph, School of Advanced Military Studies (Fort Leavenworth, KS: United States Army Command and General Staff College, 2008), 19–22.

[307] Michael T. Flynn, Rich Juergens, and Thomas L. Cantrell, "Employing ISR: SOF Best Practices," *Joint Forces Quarterly* 50 (3rd Quarter): 57, https://digitalndulibrary.ndu.edu/u?/ndupress,20540.

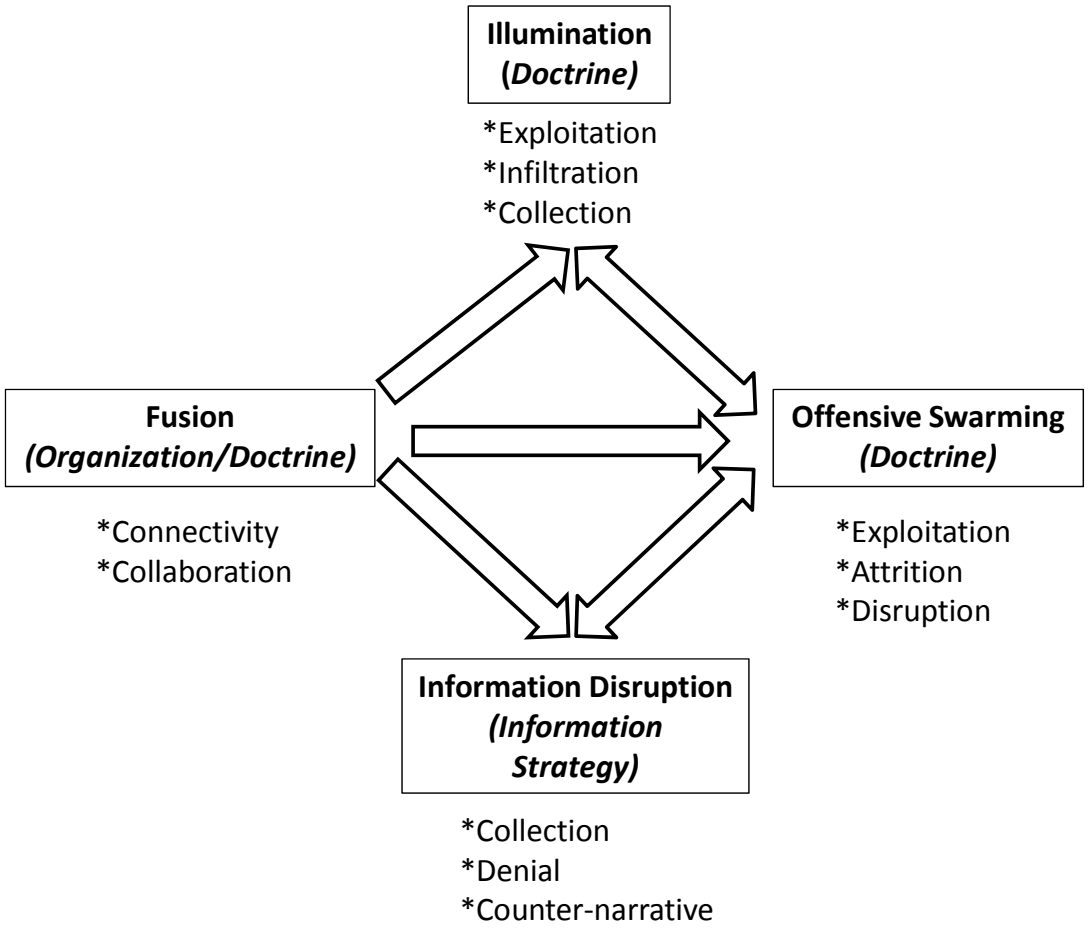

Figure 10. Variable Interaction and Associated Activities

The interaction of each of these variables is crucial and necessary, and in this regard, each variable is highly dependent on each other. Organizational design and the fusion that results from enhanced connectivity are crucial for establishing a baseline for operational activity. Such operational activity leads to illumination, which builds on each other in a reciprocal and cyclical manner. Swarming activities are only possible with a high degree of decentralization, and high levels of information, characteristics that flow from fusion and illumination. Overall, information disruption facilitates illumination efforts, and provides an overarching purpose that enhances each activity. The common thread uniting each variable is the importance of information. Whether it is connecting

through fusion to generate more information flows, gaining information through illumination activities, using information to synchronize swarming, or crafting ways to deny it to the enemy, information permeates the interaction of these variables.

5. Models for Countering Networks

An understanding of network vulnerabilities provides the best means to derive variables, which may prove effective in countering networks. As an initial test of these variables, they are evaluated in light of four models, each representing a potential method for countering networks. The first model is a traditional military approach, or the predominant method applied against irregular opponents in most conflicts throughout history. The second model is the counter-insurgency approach, which involves both classic aspects describes by one theorist as "modern warfare,"[308] and the modern COIN doctrine, as evidenced by the combined U.S. Army and Marine Corps doctrine in FM 3-24. The third method is the counter-terrorism model, which is derived from counter-terrorism practice and current U.S. doctrine. The final method is the netwar model, which describes a network-based method of conflict closely attuned to the information age. The purpose of these models is to provide a way to examine each variable further, but most importantly, to test the specific models for their effectiveness.

a. Traditional Military Model

The traditional military model is the accepted norm of nation-state warfare. This model stems from the earliest set-piece battles, and although recent advances strive for more effective maneuver, much of this mode strives for what is commonly recognized as attritional warfare.[309] Organizationally, this model is hierarchical and largely bureaucratic in nature. As a product of the Industrial Age, the traditional military structure seeks to optimize organizational performance by standardization. Henry Mintzberg describes a machine bureaucracy as consisting of a

[308] Trinquier, *Modern Warfare*, 6.

[309] Edward N. Luttwak, "Notes on Low-Intensity Warfare," *Parameters* 13 (December 1983): 335–337.

formal hierarchy built to optimize task performance in a stable and simple environment. A machine bureaucracy has rigid departmentalization, centralization or authority, and standardization of performance.[310] Since its doctrine is largely predicated on the use of direct and overwhelming force, it relies on mass formations capable of directing large numbers of men, equipment, and resources. Doctrinally, the traditional military model relies on forms of maneuver largely linear in nature, and that seek to remain on the offense. This style of warfare is largely based on the idea of attrition, or that by degrading enough of an opponent's force; it will be ineffective on the battlefield and unable to obtain its goals. Operationally, traditional militaries seek to use overwhelming force against an opponent, largely in the form of firepower. Technological advance is a primary factor in the development of weapon systems, which shapes operational methods. While seemingly backwards, this driver is somewhat understandable due to the large economic costs and development time that significant weapons require, largely determining that "fighting the kind of battle that fits one's weapons will be the most basic approach for any country in handling the relationship between weapons and combat…."[311] Information strategy tends to follow the same approach, which is focused towards attacking enemy forces. In essence, information is used to support traditional forms of warfare, rather than adapting to the powerful aspects of information in irregular conflict. Traditional militaries employ information in ways directed at targeting command and control systems, using technology to counter technology, such as electronic-based warfare, and focusing on denying the enemy access to intelligence.

All this is not to suggest that traditional warfare is static, but that instead, even the most dramatic changes, those emphasizing maneuver to achieve decisive effects, largely preserve its fundamental nature.[312] While traditional warfare methods have been increasingly modified with rapid advances in technology, leading to efforts to incorporate NCW, this step in the right direction is hamstrung by the fundamental reliance on outmoded forms of organization, doctrine, operational methods, and information strategy.

---

[310] Mintzberg, "Organization Design," 7.

[311] Lang and Xiangsui, *Unrestricted Warfare*, 11.

[312] John Arquilla, *Worst Enemy: The Reluctant Transformation of the American Military* (Chicago: Ivan R. Dee, 2008), 25–26.

It is not enough to have forces increasingly linked by modern technology if those forces are unable to take full advantage of the increased connectivity that such technology offers. While NCW provides considerable advantage against another traditional opponent, which is not networked, it is insufficient to address the fully networked-style warfare employed by fighting networks. "Compared to these adversaries [non-state warriors], professional armies are like gigantic dinosaurs which lack strength commensurate to their size in this new age."[313] While the traditional model continues to be employed against irregular opponents, past experiences in this arena highlight the requirement for dramatic changes, producing the counter-insurgency model.[314]

b. Traditional Model Evaluation

The traditional military model is designed to confront another traditional military opponent on the battlefield. It rarely performs effectively against fighting networks, providing a poor match-up against those variables necessary to counter networks. Perhaps the most compelling example of this model is the observation that the optimized traditional military that proved so successful in the invasion of Iraq, floundered dramatically as the situation gave rise to irregular warfare. Rows upon rows of tanks and armored vehicles collected dust after the initial invasion of Iraq, largely irrelevant in the fight against dispersed and concealed networks. These paragons of the traditional model, so effective in countering the formal Iraqi army, are nearly useless in the on-going low-intensity conflict. The traditional military model places a great deal of emphasis on large volumes of firepower to decimate its opponents on the battlefield.[315] Such mechanistic organization and application is not only ill-suited to countering dispersed and concealed networks, it is actually just the opposite of what is required.[316] According to van Creveld, "in fact, there are solid military reasons why modern regular forces are all but useless for fighting what is fast becoming the dominant form of war in our age. Perhaps the most

---

[313] Lang and Xiangsui, *Unrestricted Warfare*, 11.

[314] David Galula, *Counterinsurgency Warfare: Theory and Practice*, [1964] (Westport, CT: Praeger Security International, 2006), 50–51.

[315] Luttwak, "Notes on Low-Intensity Conflict," 336.

[316] Martin van Creveld, *The Changing Face of War* (New York: Ballantine Books, 2006), 222–225.

important reason is the need to look after technology on which the force depends…"[317] In light of this, its primary value in evaluation may be to provide a starting point for understanding the vastly different requirements for success in irregular warfare.

(1) Offensive Swarming. The traditional model seeks to defeat its opponent using a significant mass of forces, direct sustained combat, and decisive engagement. The traditional model forces generally attack in a linear manner, or maneuvers to achieve penetration and add depth to their advance. Although distinctly non-linear aspects, such as increased mobility, precision fires, and simultaneous operations are changing maneuver warfare, the traditional model is poorly suited to conduct offensive swarming. While swarming occurred in the past, those instances featured military elements utilizing synchronized communications and considerable command and control agility.[318] The primary organization and doctrine of the traditional model make it difficult to swarm.

(2) Illumination. The key aspects of illumination stem from the irregular warfare environment and the traditional model places little emphasis on its requirements. While fighting networks are concealed, a traditional enemy is usually fairly definable and the larger questions center on how it will maneuver and what capabilities it will employ. Traditional armies feature fairly set and establish "order-of-battle" organizational structures, with each branch focuses on its role in confronting the enemy. Intelligence in the traditional model is primarily focused on understanding what the enemy's intentions are, and how it will maneuver on the battlefield, much less than who and where they are. The emphasis on social ties and infiltration required to understand networks is not considered when dealing with traditional opponents.

(3) Info Disruption. The traditional model may conduct information disruption, but it is usually an area of secondary emphasis. It places more reliance on information warfare aspects, such as command-and-control warfare, and electronic warfare than it does on understanding a network's information strategy and

[317] Creveld, *The Transformation of War*, 118.

[318] Edwards, *Swarming and the Future of Warfare*, 82.

seeking ways to disrupt it. With a primary emphasis on decisive battle, the traditional model seeks to confront an enemy opponent directly, rather than focus efforts on collection. Information operations are usually geared towards general propaganda efforts, which may be effective, but are usually not synthesized with military action.

(4) Fusion. The traditional model places a large degree of emphasis on (C2, but now expanded to include command, control, communications, and computers, as well as ISR—C4ISR), and the systems that facilitate achieving information superiority and control. While a primary aspect of fusion is the connectivity and shared system it requires, fusion requires organizational changes and a system that promotes fusion to be effective. The hierarchical structure that dominates much of the traditional model reinforces vertical structures that limit connectivity and cannot achieve a fusion-based system.

c. Counter-Insurgency Model

The counter-insurgency model describes the response by nation-states to those that threaten them, which often takes the form of a struggle for legitimacy and control, the authority and ability to take action, with respect to a population. With the conflicts in Iraq and Afghanistan, "counter-insurgency is fashionable again: more has been written on it in the last four years than in the last four decades."[319] Much of what is written and debated about COIN centers on the proper response to insurgent threats, and has formed as significant part of an ongoing national security debate.[320] Internal to the counter-insurgency model are two aspects of it that are generally described as the classic form, and the new form "popularized" and formalized in U.S. military COIN doctrine. With the idea of state-building receiving closer scrutiny, counter-insurgency as a whole is "…moving away from viewing threats to states through 'Maoist' models of competition toward a wider appreciation of decentralized networks and criminal insurgency."[321] It may be that currently known classic notions of insurgency are changing altogether,

[319] Kilcullen, "Counter-Insurgency Redux, 111.

[320] Lynch III, "Conceptual and Operational Challenges of COIN," 6.

[321] Sullivan and Elkus, "Strategy and Insurgency," 1.

departing from both the classical model and modern U.S. military COIN approaches. Regardless, the counter-insurgency model continues to serve as a framework for efforts to counter fighting networks.

Classic counter-insurgency is largely a product of "small wars," and their revolutionary descendants of the last century. The classical model seeks to incorporate the historical depth in strategic thought and practice of irregular warfare. While counter-insurgency has its roots in small wars and timeless low-intensity conflict, recently, it has been interpreted as a response to political strategy.

Organizationally, the classic counter-insurgency model is based on devoting the minimum amount of resources to dealing with an irregular opponent. Since counter-insurgency is largely about forcing an adversary to accept the state's political control, classic counter-insurgency uses military and police forces to counter irregular opponents. In this way, counter-insurgents organized and applied a similar doctrine to that of their guerrilla opponents, leading to an extensive focus on counter-guerrilla doctrine. Successful counter-guerrilla efforts were notable for their similarities to guerrilla warfare techniques. "Guerrillas and counter-guerrillas alike, resembling hostile brothers, must be masters in the art of organizational infiltration."[322] Doctrinally, counter-insurgents must also fight like those they face. "Basically this simply means that the measures devised and used against guerrillas, saboteurs and spies take on much of the *modus operandi* of the guerrilla."[323] Counter-insurgents also recognized the importance of the population and focused measures on how to ensure the populations cooperation.[324] Operationally, most successful counter-insurgent forces are light infantry or special operations type forces, which are able to pursue withdrawing insurgents following their hit-and-run attacks.[325] More indirect measures focus around rationing and controlling the population to halt critical resources of food and munitions. Information strategy is

[322] Gann, *Guerrillas in History*, 78.

[323] Virgil Ney, *Notes on Guerrilla War: Principles and Practices* (Washington, DC: Command Publications, 1961), 121.

[324] Galula, *Counterinsurgency Warfare*, 52.

[325] Ney, *Notes on Guerrilla War: Principles and Practices*, 129.

focused on external information meant for the global audience, and local information, which is focused against the insurgent forces. The major focus of this information strategy is to win the active support of the population and to deprive the insurgent of that support.

> Above all, counter-guerrilla forces must convince their opponents that resistance is hopeless, that the guerrilla leadership is selfish, incompetent, corrupt, and divided, that surrender will bring neither dishonor, torture, nor death, and that capitulation is the only rational policy. This task is essential in the battle for the minds of the civilian population. The government forces should, at the same time, attempt to sow dissension among the enemy and should not disdain bribery where necessary.[326]

Modern U.S. military COIN doctrine and the practices that have evolved since the recent wars in Iraq and Afghanistan, focus on the population as the "center of gravity." Ideas derived from French and British experiences in the 1950s, most notably David Galula's work, *Counterinsurgency Warfare: Theory and Practice*, have been interpreted through Cold War experiences and support operations to produce counter-insurgency theory with a principal focus on the needs of the population. The U.S. Army relooked its views on irregular warfare in the face of a losing insurgency in Iraq in 2006, and General David Petraeus and others produced a new doctrine in the form of Field Manual 3-24, *Counterinsurgency*. This modern COIN doctrine is widely credited with being operationalized in the surge of forces that many credit with restoring stability to Iraq.[327] According to FM 3-24, "at its core, COIN is a struggle for the population's support. The protection, welfare, and support of the people are vital to success. Gaining and maintaining that support is a formidable challenge."[328] However, it is critical to understand that the ideas forming modern COIN are based on a limited number of

[326] Gann, *Guerrillas in History*, 85.

[327] Gorka and Kilcullen, "An Actor-Centric Theory of War," 14.

[328] U.S. Department of Defense, Field Manual 3-24, *Counterinsurgnecy*, 1–28.

examples in the recent past, and framed in a nation-building format; used as a tool for seeking a "drastic alteration of political, economic, and social structures, a forcible reengineering of a nation."[329]

Organizationally, COIN seeks to use conventional military forces as the primary tool for restoring security and providing stability. While stressing unity of effort between civilian and military organizations, "command and control of all U.S. Government organizations engaged in COIN missions should be exercised by a single leader through a formal command and control system."[330] While the primary forces described are dismounted infantry and special operations, there is little mention of the organization of these elements, and traditional command structures remain.

Doctrinally, the current interpretation of COIN seeks to provide "techniques and procedures [which] can keep U.S. forces more agile and adaptive than their irregular enemies."[331] Much of COIN doctrine focuses on the ability to integrate disparate governmental agencies, military organizations, and non-governmental organizations (NGOs). Intelligence plays a major factor in COIN, with an emphasis placed on the populace, host nation, and insurgents.[332] Overall, all actions are taken together with a host nation government that seeks to counter the insurgent's strategy and maintain the government's legitimacy.

Operationally, COIN operations flow in three phases that seek to first protect the population, break the insurgents' momentum, and establish further engagement; second, achieve stability; and finally, expand stability and transition responsibility to host nation control.[333] Operations focus on intertwining combat, civil security, essential services, governance, and economic development into a cohesive

[329] Gorka and Kilcullen, "An Actor-Centric Theory of War," 16.

[330] U.S. Department of Defense, Field Manual 3-24, *Counterinsurgency*, 2–2.

[331] Ibid., ix.

[332] Ibid., 3–1.

[333] Ibid., 5–2.

overall effort.[334] Operations may be conducted in the form of clear-hold-build, combined action with host nation forces, or limited action in support of a host nation's efforts.[335]

Information strategy in COIN is focused on information operations that support the overall effort and each line of operation being conducted. COIN doctrine describes information operations as often the decisive line of operation, which is fundamentally required to shape the information environment. In addition, COIN seeks to implement functional information engagement at the local level, in personal interaction. "Face-to-face interaction by leaders and soldiers strongly influences the perception of the local populace," and according to Field Manual 3-0, may be "critical to mission success."[336]

Overall, the current COIN model in practice today represents a dramatic leap forward in attempting to formulate a method for addressing the complex dynamics surrounding insurgencies. Notably it incorporates the use of social network analysis in a basic form, and explains its importance in understanding the myriad networks that COIN practitioners face.[337] COIN is primarily focused on addressing a broad insurgency movement that requires the support of the population that centers on counter efforts that seek to win "hearts and minds."

d. COIN Model Evaluation

Counter-insurgency and its modern variation, COIN doctrine, are specifically tailored as responses to irregular opponents—those launching an insurgent movement against another authority. Fundamentally, the current COIN model is a response to a popular-based insurgency that utilizes guerrilla warfare as a primary source of tactics in a struggle for control. Its application requires an understanding beyond just the recent U.S.-led conflicts. More importantly, "…we need to be aware of the fact that

---

[334] U.S. Department of Defense, Field Manual 3-24, *Counterinsurgency*, 3–24, 5–6.

[335] Ibid., 3–24, 5–18—5–25.

[336] U.S. Department of Defense, Field Manual 3-0, *Operations* (Washington, DC: U.S. Government Printing Office, 2008), 7–4.

[337] U.S. Department of Defense, Field Manual 3-24, *Counterinsurgency*, B–10—B–17.

COIN—in the American mode—is but one small reflection of the much older, even ancient, practice of countering insurgents, or irregular enemies."[338] It may very well be that the "…constricted foundations upon which classical COIN doctrine was built have not only distorted our understanding of the current threat environment, but also dangerously limits our ability to defeat current and future enemies."[339] The strengths of COIN make it a valuable model and provide a doctrine for countering insurgent networks. However, because of its overarching focus on popular support, COIN devotes relatively little attention to how to counter increasingly complex, globalized, and information-savvy fighting networks. It has limited utility in situations in which popular support is either not possible, or a secondary aspect. Another aspect is the relationship of tangible support and population support. When support for insurgents comes from the population, the popular support is the center of gravity. However, if the insurgent's tangible support is not reliant on the population, then an effective counter-insurgent campaign should focus on other areas.[340] An example of this type of campaign is the increasing violence employed by trans-national terrorist and criminal networks.

(1) Offensive Swarming. COIN doctrine seeks to establish a strong link with the local population and makes this the primary effort. Establishing local services, security, and "winning hearts and minds" are very different than, and perhaps conflict with, offensive swarming. Local security requires forces dedicated to providing a stable security presence at the local level. In this regard, COIN doctrine provides little discussion of how to maneuver against insurgents offensively, and focuses instead on population-based efforts. However, it may be that offensive actions are not necessarily incompatible with local security, and that COIN could place more emphasis on aspects required to disrupt violent networks. This aspect would be imperative in situations in which an irregular opponent is strong enough to counter local security efforts, or in a high-intensity environment, which threatens COIN forces. The later situation requires

[338] Gorka and Kilcullen, "An Actor-Centric Theory of War," 15.

[339] Ibid.

[340] Paul, Clarke, and Gill, "Victory Has a Thousand Fathers," 6.

something beyond COIN fundamentals designed for "low-intensity conflict," a way of countering extremely capable opponents while balancing a population-centric approach.

(2) Illumination. Classic counterinsurgency places significant emphasis on the use of intelligence to understand who the guerrillas are and what amount of support they receive. Modern COIN doctrine addresses the tremendous intelligence required to counter an insurgency, but focuses primarily on intelligence derived from the local population. In fact, this doctrine is the stated primary purpose of some of the most insightful COIN thinking. John Nagl states, "the prime requirement for a successful military component of a counterinsurgency effort is intelligence derived from a supportive population."[341] The "Diamond Model," described by Gordon McCormick, emphasizes the need to obtain information on the insurgents from the population, as the primary means to counter the guerrilla's information advantage.[342] However, it is critical to determine the level of support the insurgents have from the population and their ability to be recognized within it. If the locals have little intelligence on the enemy, then the only ones with a preponderance of information about the enemy are themselves. This situation appears to be increasingly common, as popular-based rural insurgents give way to fighting networks that may require little public support, and whose ability to move and communicate is not necessarily tied to terrain or local conditions. Given these conditions, exploitation from within the network becomes critical to understanding and knowing the enemy, and is more effective than information from local sources.

(3) Information Disruption. Classic counter-insurgency recognizes the information aspect of an insurgency, but in a local context. Psychological operations are focused on this aspect, and "effective counterinsurgents use information operations (IO) to exploit inconsistencies in the insurgents' message, as well as their excessive use of force or intimidation. The insurgent cause itself may also present vulnerabilities. Modern counterinsurgents may be able to "capture an insurgency's cause

---

[341] John Nagl, "Strategic Innovation: Integrating National Power to Win in Iraq," in *Ideas as Weapons: Influence and Perception in Modern Warfare*, ed. G. J. David Jr. and T .R. McKeldin, III (Dulles, VA: Potomac Books, Inc., 2009), 95.

[342] McCormick, "Diamond Insurgent/COIN Model," 6.

and exploit it."[343] Modern COIN places a significant emphasis on information operations, but most of these are of a positive nature, and seek to address issues vis-à-vis the population. Little recognition of the insurgent's information advantages occurs, and efforts to counter them are either downplayed or not mentioned. In addition, the tension that exists between a largely traditional, specialized military and the "…increasingly complex social dynamics and political operations…" of modern COIN add to the difficulties of conducting information disruption.[344]

(4) Fusion. Aspects of fusion are evident in certain areas of the COIN model, and classic counter-insurgency provides several early attempts at fusion, most notably the British Special Police efforts in Malaya. Recent experiences in Iraq and Afghanistan, notably the intensive efforts between conventional and special operations forces in the former, show the importance of collaborative effort. However, the COIN model provides a cooperative relationship between different units and agencies rather than any kind of fusion system. While collaboration is encouraged and recognized as essential, connectivity is not fully present, and little discussion of a comprehensive system within the COIN model occurs. COIN focuses on the effective passing of intelligence, gained primarily from the population, to operational forces. The decentralized, tactical nature of COIN provides for elements of fusion at the tactical levels, with patrols gathering local intelligence and then acting on that information.

e. Counter-Terrorism Model

Counter-terrorism is a response to the increase in terror tactics employed within irregular warfare. While terrorism is as timeless as human conflict, a modern resurgence of terrorism appeared in revolutionary struggles over the last century. By the 1970s and 1980s, terrorism filled the global environment due to technological advances and an increase in media coverage, as well as covert sponsorship from such countries as the Soviet Union, Iran, and Libya.[345] By the late 1990s, four trends in modern terrorism

[343] U.S. Department of Defense, Field Manual 3-24, *Counterinsurgency*, I–18.

[344] Rid and Hecker, *War 2.0*, 78.

[345] Cronin, "Behind the Curve," 37.

appeared: an increase in religiously motivated attacks, decrease in overall attacks, increased lethality; and increase in the targeting of Americans.[346] These trends produced little change in an overall response-based view towards counter-terrorism, one that was generally poised to react to an incident or specific threat. Counter-terrorism capabilities supported a law enforcement focus, but consisted of "…specialized, but limited, military CT capabilities to rescue hostages, take preemptive action or retaliate against terrorists because they were geographically or politically beyond the reach of law enforcement."[347] The 9/11 attacks changed the overall view of counter-terrorism, which has primarily focused on military actions against entire terrorist networks, action that expanded from a law-enforcement or select special operations focus to a more comprehensive focus. Counter-terrorism is now generally understood to be a two-pronged strategy, focused on direct strikes against terrorists themselves, and an overall policy that addresses the economic, ideological, and religious aspects that promote and sustain terror networks. In recognition of these changes, the U.S. Department of Defense produced its newest joint publication on CT, defining it as "actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks."[348]

Organizationally, CT is the primary focus of Special Operations Forces (SOF) and other paramilitary units that conduct direct and surgical action against a specific terror threat or terrorist targets. These units tend to be small, but highly resourced, and are supported by their larger military structures. Since CT operations tend to be of national-strategic importance, they are highly scrutinized and fall under a formal, hierarchical chain of command. Individual SOF units that conduct these operations may be fairly decentralized and operate with a great deal of autonomy, but their operations are traditionally subject to a great deal of oversight and control.

---

[346] Cronin, "Behind the Curve," 42.

[347] U.S. Department of Defense, Joint Publication 3-26, *Counterterrorism*, I–1.

[348] Ibid., I–2.

In general, CT doctrine is primarily deterrence focused, with the ultimate aim of raising the costs to terrorists of launching attacks.[349] Within this deterrence framework, however, CT emphasizes offensive actions against terrorist networks, whether direct or indirect. The U.S. strikes against al-Qaeda training camps in Afghanistan during Operation Enduring Freedom provides a noteworthy example. These attacks reflected a U.S. policy shift following 9/11 towards prevention, which promotes a larger offensive focus to "…initially disrupt, over time degrade, and ultimately destroy terrorist organizations."[350] This policy remains, and contains a core element focused on pre-empting signs of terror attacks, as seen in the current National Military Strategy, released in February, 2011, "undeterred by the complexity of terrorist networks and in concert with our Allies and partners, we will be prepared to find, capture, or kill violent extremists wherever they reside when they threaten interests and citizens of America and our allies."[351] The same document continues to state that these efforts must complement an indirect approach that focuses on economic development, governance, and rule of law.[352]

Operationally, much of the nature of CT is encapsulated in a high degree of secrecy. From recent examples, such as the direct strikes against terrorists in the current conflict with al-Qaeda, it is clear that SOF units primarily undertake these actions, but, as joint doctrine states, they also rely on interagency and conventional military support to a great degree.[353] Despite having small units, which operate using traditional SOF principles, an overall high degree of coordination and information sharing surrounding CT operations occurs. These collaborative aspects apply to both the direct and indirect operational approaches, which provide CT operations with a high degree of operational fusion.

---

[349] Ivan Sascha Sheehan, *When Terrorism and Counterterrorism Clash* (Youngstown, NY: Cambria Press, 2007), 50.

[350] George W. Bush, *The National Strategy for Combating Terrorism* (Washington, DC: The White House, February 2003), 2.

[351] U.S. Joint Chiefs of Staff, *The National Military Strategy of the United States*, February 8, 2011, 6.

[352] Ibid., 7.

[353] U.S. Department of Defense, Joint Publication 3-26, *Counterterrorism*, III–9—III–13.

Counter-terrorism requires a comprehensive information strategy, for both direct and indirect actions. Much of the emphasis in the area is placed on psychological operations, which are "…used to discredit the terrorist activities and to show the benefits of rejecting terrorism and its associated activities in an effort to gain popular support for the CT operations."[354] However, it is unclear whether an information strategy exists to comprehensively address the reality that, "…in the age of mass electronic media terrorism is undoubtedly an act of communication. In many respects, the pervasiveness of the 24/7 news cycle makes the media one of the single most important components of the current dynamics of terrorism and counterterrorism."[355]

f. CT Model Evaluation

The CT model is based on the majority of global counter-terrorism practices and current U.S. military doctrine. Historically, CT has focused on attacking terrorist organizations and providing a response to the threat of terror attacks. Since 9/11, CT has served both as an operational distinction, but also as an overall strategy, and as a different approach from the population-centric nature of COIN. In this manner, CT is commonly understood as an approach that seeks to attack a terrorist network directly. CT recognizes that terrorist organizations have vulnerabilities, and it offers a rich history of experiences and indicators of success against terrorist organizations.[356] More recent approaches are defining the cutting-edge of warfare and providing new examples of techniques, organizational approaches, and doctrinal innovation. The Joint Special Operations Task Force (JSOTF) led by General Stanley McChrystal adopted the premise posed by Arquilla and Rondfeldt in their numerous writings on netwar and it became their mantra—"it takes a network to defeat a network." McChrystal claims that, "as our operations in Iraq and Afghanistan intensified, the number of operations conducted each

---

[354] U.S. Department of Defense, Joint Publication 3-26, *Counterterrorism*, III–7.

[355] William C. Banks, Renée de Nevers, and Mitchel B. Wallerstein, *Combating Terrorism: Strategies and Approaches* (Washington, DC: CQ Press, 2008), 268.

[356] Christopher C. Harmon, "Vulnerabilities of Terror Groups," *Lexington Institute*, March 2007, 2, www.lexingtoninstitute.org.

day increased tenfold, and both our precision and success rate rose dramatically."[357] The CT model employs operational swarming, focuses on illuminating a terrorist network, and incorporates fusion in a systematic way. The CT model, as currently employed, utilizes many of the tenets of network-based operations, and by all accounts, appears to be fairly successful against fighting networks in Afghanistan and Iraq.

(1) Offensive Swarming. While CT units are composed of smaller elements, their overall small size and limited scope has traditionally limited their employment to specific crisis-response missions. It would appear that CT units could conduct offensive swarming if employed in such a way that maximized their numbers. The CT model clearly provides for achieving surprise, which is a fundamental characteristic of the manner in which these SOF units operate. Operational tempo seems difficult to achieve given the small number of CT units, especially when they are facing a large network. However, indications from recent CT efforts show that it may be very possible, as McChrystal's statements imply an extremely high rate of operations.[358] Pulsing could be achieved as well, if intelligence were the driving factor in controlling the operational nature of CT, and operations focused on gaining the most decisive effects against the network.

(2) Illumination. The CT model focuses specifically on terrorist networks and looks for operational activity to find and illuminate aspects of a terrorist network. Terrorism, despite its intentionally visible acts, is largely a hidden threat; the fighting networks that employ it make full use of concealment, and are increasingly more diffuse and amorphous. For this reason, and because the doctrinal innovation that terrorists employ results in such catastrophic attacks, counter-terrorism places more emphasis on intelligence than the other models examined. Many of the techniques used to illuminate networks stem from law-enforcement use in combating terrorism. Recent uses have employed an examination of social ties, but it is possible that more could be done in this arena. While considerable activity is placed against understanding the terrorist network, much less effort is devoted to understanding the full

[357] McChrystal, "It Takes a Network: The New Frontline of Modern Warfare," 4.

[358] Ibid., 6.

range of social networks, which support and create the strong ties in these networks. This is not the rule, though, and some countries place extensive emphasis on the social roots of terrorism.[359]

Infiltration generally takes considerable effort, both in the use of classic espionage and pseudo-operations, but it is a "high-payoff" activity. It is widely believed that HUMINT capabilities are lacking, and that an increased focus on less-technical means, such as basic espionage and developing human-based knowledge, can provide better illumination opportunities than just technical collection.[360]

Recent counter-terrorism activities increase the emphasis on operational activity, and use the timeless lesson that the operational activity of terrorist networks exposes them to scrutiny.[361] Dedicated intelligence work uses all forms of intelligence to collect on operational activity, and the German's comprehensive approach to dealing with the Baader-Weinhof terrorist group provides an excellent example, as it "…featured great intelligence and superb police effort. A new office for criminal investigation based in Wiesbaden employed scores, and then hundreds, and then thousands of data specialists, running unprecedented computer profiling efforts."[362] Technical collection comes to the fore in the CT model when pin-pointing, tracking, and analyzing this operational activity.

The CT model stresses the importance of exploitation, and it is a significant aspect of the targeting cycle. As exploitation fundamentally concerns gaining intelligence about an opponent's network, it provides the primary means for illumination in CT operations. This emphasis provides a "feedback loop" that enables both horizontal and vertical information sharing and is so important that it is being emulated by elements throughout the military.[363]

---

[359] Ian O. Lesser, "Countering the New Terrorism: Implications for Strategy," in *Countering the New Terrorism*, ed. Ian O. Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt, and Michele Zanini (Santa Monica, CA: RAND, 1999), 118.

[360] Berkowitz, *The New Face of War*, 200–208.

[361] Harmon, "Vulnerabilities of Terror Groups," 2.

[362] Ibid., 3.

[363] Hartman, "Exploitation Tactics," 19.

(3) Information Disruption. The CT model places less emphasis on information disruption than it does on the other variables. Negating an opponent's purpose is an indirect approach to countering terrorism, and while it receives attention, it is secondary to the direct efforts of the other variables. However, information disruption is still present, primarily in efforts to collect on communications. Such efforts could be expanded dramatically with a greater focus on information strategy. Overall, the lack of such strategy appears to be a glaring weakness in the current CT model.[364]

(4) Fusion. The CT model places a significant emphasis on fusion and recognizes that operations and intelligence must be combined and united in their efforts. Much of the recent emphasis on interagency cooperation discusses fusion cells as an organizational form and also a means to ensure that vast and complex streams of intelligence regarding terrorist threats. In this regard, CT addresses fusion both organizationally and doctrinally. In recent counter-terrorism efforts, "operators and analysts from multiple units and agencies sat side by side as we sought to fuse our intelligence and operations efforts—and our cultures—into a unified effort."[365] The doctrinal element is possible through a collaborative network between operational elements and intelligence analysts. This collaboration reflects a doctrinal insight developed in response to the challenge of fighting networks in both Afghanistan and Iraq, challenges that required "…achieving levels of knowledge, speed, precision, and unity of effort that only a network could provide."[366] As McChrystal explained:

> This insight allowed us to move closer to building a true network by connecting everyone who had a role—no matter how small, geographically dispersed, or organizationally diverse they might have been—in a successful counterterrorism operation. We called it, in our shorthand, F3EA: find, fix, finish, exploit, and analyze. The idea was to combine analysts who found the enemy (through intelligence, surveillance, and reconnaissance); drone operators who fixed the target; combat teams who finished the target by capturing or killing him;

[364] Doorey, "Waging an Effective Communications Campaign in the War on Terror," 150–155; LTC James McNeive, "Frustration," in *Ideas As Weapons: Influence and Perception in Modern Warfare*, ed. G. J. David Jr. and T. R. McKeldin III (Washington, DC: Potomac Books, 2009), 357-361.

[365] McChrystal, "It Takes a Network: The New Frontline of Modern Warfare," 6.

[366] Ibid., 2.

> specialists who exploited the intelligence the raid yielded, such as cell phones, maps, and detainees; and the intelligence analysts who turned this raw information into usable knowledge. By doing this we speeded up the cycle for a counterterrorism operation, gaining valuable insights in hours, not days.

This fusion system is clearly a doctrinal innovation, developed within the CT model, and is emphasized in organizations that face complex, highly adaptive, networked threats.

g. Netwar Model

The netwar model focuses on the revolutionary changes in the modern information age and the recognition, rise and use of networks as a powerful element that is not addressed in current terms seeking to describe irregular warfare and low-intensity conflict.[367] "The term 'netwar' connotes that the information revolution is as much about organizational design as about technological prowess, and that this revolution favors whoever masters the network form."[368] It is important to distinguish that the netwar model focuses on an emerging mode of conflict that emphasizes social conflict, much of which occurs short of traditional warfare.[369] In this regard, some of the attributes of netwar may be more applicable in discussions of social conflicts and criminal activities, but most remarkably describe the revolutionary blend of activity occurring in irregular warfare. Many of netwar's attributes are found in the description of how networks fight, but will be highlighted in this study to present a model for countering fighting networks.

Organizationally, networks are composed of nodes of various size and activity. The nodes in netwar are robustly linked in various structural combinations, but trend towards all-channel formation, with multiple linkages forming a robust network form. Netwar actors "…generally consist of dispersed, often small groups who agree to

[367] Arquilla and Ronfeldt, *The Advent of Netwar*, 7.

[368] Ibid.

[369] Ibid., 5.

communicate, coordinate, and act in an internetted manner, often without precise central leadership or headquarters. Decision-making may be deliberately decentralized and dispersed."[370]

Doctrinally, netwar provides for both offensive and defensive actions in ways remarkably adaptable. This adaptability allows for a unique transition and even blending of offensive and defensive actions. Swarming is a distinct reflection of this attribute, and it involves self-synchronized nodes or cells able to attack en-mass, but utilize dispersion to provide for tremendous resiliency.[371]

Operationally, netwar focuses on fluid attacks that seek a decisive effect. Often, networks attack in a pulsing manner with cycles of collecting information and waiting, then decisive attacks. Networks may benefit from the inaccessibility that physical terrain provides, but the networked form allows them to achieve concealment in ways that largely reduce the need for a purely physical safe havens. The cyber environment provides another way to achieve concealment.

Netwar is primarily about understanding the dynamics of the information age and seeks to dominate information strategy throughout the conflict. Networks go beyond such focused distinctions as "winning hearts and minds," and use information as a powerful lever against their opponents. In fact, netwar as a whole tends to place more emphasis on information strategy than it does on actual conflict.

h. Netwar Model Evaluation

The Netwar model is based on the use of the network form as an organizational and doctrinal innovation uniquely suited to conflict in the information age. One of its key propositions is that "it takes networks to fight networks," leading to an understanding that, "…those who want to defend against netwar will, increasingly, have to adopt weapons, strategies, and organizational designs like those of their

[370] Arquilla and Ronfeldt, *The Advent of Netwar*, 5.

[371] Edwards, *Swarming and the Future of Warfare*, 2.

adversaries."[372] The netwar model provides a framework for analysis that includes organizational, doctrinal, technology, narrative, and social dimensions, covering the primary aspects of the challenges displayed by fighting networks in the information age. Bruce Berkowitz succinctly states, "…the information revolution has fundamentally changed the nature of combat. To win wars today, you must first win the information war." The netwar model is primarily tailored to this new nature of combat, and depicts noteworthy operations, such as al-Qaeda's attack on the *USS Cole*, the 9/11 attacks, and U.S. SOF and CIA paramilitary units' initial operations against the Taliban. Each of these recent examples of combat involved "small cells, dropped into the middle of hostile territory," that "…coordinated their operations both with each other and with their commanders back home, thousands of miles away."[373] The emphasis in the netwar model is on the ability of dispersed nodes to communicate and coordinate, and the organizational and doctrinal attributes that make such activity possible.

(1) Offensive Swarming. Networks whose primary doctrinal approach is swarming define the netwar model. While the netwar model emphasizes a blurring of offense and defense, overall netwar signals an offense-dominant era, with "greater disruptive power in small units."[374] As previously discussed, the basic characteristics of swarming are decentralization and high information flows, both of which are strongly emphasized in the netwar model. While the netwar model does not specifically address aspects, such as operational tempo, it is apparent that it could incorporate such features.

(2) Illumination. Netwar identifies the challenge of finding networked opponents, and places an emphasis on intelligence that allows for detection, prevention, and tracking. While detection and tracking are clearly aspects of illumination, illumination as a core activity is not fully developed in the netwar model. The reason for this appears to be the primary focus on social aspects of netwar instead of irregular

[372] Arquilla and Ronfeldt, *The Advent of Netwar*, 82.

[373] Berkowitz, *The New Face of War*, 108.

[374] Arquilla and Ronfeldt, *The Advent of Netwar*, 93.

warfare. However, the concepts underlying netwar, and the irregular conflict it describes, provide a framework for further development, and operational catalysts continue to advance these concepts, as evidenced in the CT model.

(3) Information Disruption. Netwar places a primacy on the information dimension of conflict. It is a concept deduced from the "…effects and implications of the information revolution," and "…helps show that evidence is mounting about the rise of network forms of organization, and about the importance of 'information strategies' and 'information operations' across the spectrum of conflict…"[375] Netwar discusses monitoring, targeting information flows, and safeguarding information technology infrastructure.[376]

(4) Fusion. While the netwar concept does not explicitly discuss fusion, its key implication is that effective netwar will require interagency mechanisms and operations.[377] The intent is clearly to provide for a level of collaboration between various organizations and efforts, emphasizing that "…efforts at counternet-war should be grounded in interagency cooperation (a variant of 'jointness')."[378] Fusion describes an operational system that facilitates this interaction, which starts with a merging of operational and intelligence-based efforts.

6. Model Comparison

Overall, the models "performed" largely as expected in a strict comparison test. The test is notionally based using primary characteristics from each model, and each variable is considered with the same weight. Additionally, the model comparison highlights some interesting aspects and recent developments that contribute to countering fighting networks.

---

[375] John Arquilla and David Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwar*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND, 2001), 19.

[376] Zanini and Edwards, "The Networking of Terror in the Information Age," 55.

[377] Arquilla and Ronfeldt, *The Advent of Netwar*, 81.

[378] Ibid., 85.

	Offensive Swarming	Illumination	Info Disruption	Fusion
Traditional Model	1	0	1	0
COIN Model	1	2	1	1
CT Model	2	3	1	3
Netwar Model	3	2	3	2
Scale: 0—Not effective 1—Somewhat Effective 2—Effective 3—Highly Effective				

Table 3. A Comparison of Model Performance with Counter-Network Variables.

The traditional model exhibits little to no capability to perform against a networked opponent. The reasons for this deficiency lie primarily in the organizational and doctrinal aspects of the traditional model. Despite an increasing emphasis on technology, the hierarchical and mechanistic nature of traditional militaries continues to limit their performance in the information age. The hierarchical structure and fairly centralized C2 limits the traditional model's ability to conduct synchronized swarming, and certainly not with the agility to conduct pulsing attacks. Information disruption takes the form of information warfare and is primarily focused on disrupting another military's C2 or electronic communications systems.

The COIN model performs better than the traditional model, by recognizing the population-based dimension of irregular conflict, and seeking to influence it. However, the COIN model makes this a primary dimension, which may work when countering a popular-based insurgency, but provides little in the way of addressing networked-opponents that do not require popular support. The COIN model provides for a degree of swarming, but counter-insurgents traditionally have a difficult time balancing offensive operations against insurgents with the larger requirement to win hearts and minds. In fact, some COIN practitioners would argue that the former is damaging, and even perhaps incompatible with the latter. At the least, active measures are taken to ensure that direct

offensive operations do not produce results that damage popular support.[379] COIN also provides for a degree of illumination, by placing an emphasis on intelligence. However, few systematic examples of fusion or comprehensive illumination models exist as evident in COIN literature or practices. While performing better than the traditional model, the COIN model performs marginally overall.

The CT model addresses the challenge of countering fighting networks more effectively than either the traditional model or the COIN model. It places an emphasis on each variable, and achieves greater success with each one of them than either the previous two models. While CT originated as a reactive response to a growing terrorist threat, it has clearly changed in response to the revolutionary threats posed by networked opponents. The CT model utilizes aspects of netwar, which indicates some overlap, and builds on the primary principle that the networked organizational form is particularly well suited for information age conflict. It conducts offensive swarming, but may be limited in its capacity to do so due to the small size and limited nature of CT. However, a high operational tempo may achieve swarming-like effects, particularly if it is focused with effective illumination efforts. CT places a primary emphasis on illumination, as its fundamental purpose evolved from reacting to pro-actively countering clandestine threats. Recent discussions of SOF conducting counter-terrorism focus on an increased emphasis on operational activity and exploitation, but less emphasis occurs on utilizing social ties to illuminate and conducting effective infiltration. Information disruption is not a primary focus of CT, although it is present, primarily in the form of collection. Fusion appears to be most effectively addressed by the CT model, as it uses network-based principles to create both organizational and doctrinal innovations.

The netwar model is clearly based on the concept of networks in conflict. More than any of the other models, it emphasizes the importance of networked-based organizational forms, emphasizing networks as a unique and empowered structure. The reason for this emphasis is the changing dynamics of the information age; dynamics that netwar addresses in a revolutionary way. More than any other existing model, the netwar

[379] A model that seeks to evaluate such activity is found in MAJ Michael J. McGuire, *Modeling the Effect of Direct Action Operations on an Insurgent Population* (Newport, RI: Naval War College, 2008).

model provides a conceptual basis for addressing the vulnerabilities posed by fighting networks. The swarming concept is a doctrinal aspect of the netwar model, which proposes that it is equally effective in both offensive and defensive applications. The netwar model also provides the pulsing technique, which appears to work well as a component of swarming, and may be most effective against clandestine networks. The netwar model provides tools and perspective used in illumination efforts, most notably, social network analysis. However, it does not fully address the concepts of infiltration and exploitation. Information disruption is a key part of the netwar model, and it focuses on information strategy as a defining aspect of countering networks. The netwar model provides the most comprehensive focus on addressing fighting networks' overall purpose. Fusion provides the capability for countering networks, and draws it strength from network organization. However, while the netwar model provides the initial basis for organizational fusion, the doctrinal and systematic aspects are not fully present.

The comparison of the models reveals strengths and weaknesses within each model, but when viewed in a comprehensive manner, they reflect the potential for an initial theory of counter-network operations. While the variables are not weighted, because their overall effectiveness is due to their synchronization, some may be more important that others when facing different types of networks. The primary aspect of this theory is exposition of the organizational principles and doctrinal elements present in netwar. In addition, netwar comprehensively addresses information strategy. While netwar provides some basic tools for illumination, this activity is more fully developed, and "operationalized" in the CT model. In addition, the CT model proposes and uses fusion in ways that neither of the other models addresses, to include netwar. Netwar provides the basis for organizational fusion, shared intent, and increased connectivity, while the CT model provides doctrinal innovations in the form of collaborative systems. The netwar model provides the best overall framework for countering networks, and its basic concepts have been enhanced by operational innovations in the CT model. Based on this comparison, the fundamental aspects of effective counter-network operations derive from the netwar model, while operational design and innovations present in the CT model provide further enhancement.

C. COUNTER-NETWORK FRAMEWORK

The variables provide the initial shape of essential elements in countering networks, and the model evaluation serves as an intermediate stage in the formulation of a counter-network framework. The development of a counter-network framework is a challenging task, given the numerous factors that govern and shape network development, as well as the inherent differences in context wherever network-based conflict occurs. Networks, by virtue of their fundamental properties, are often self-generating, and highly adaptive.[380] Their adaptive nature produces a unique flexibility among organizational forms, and the doctrine employed by fighting networks matches such characteristics. Countering this flexibility requires an organizational types and a doctrinal approach able to flex and shift as rapidly as the network it faces.

The framework proposed in this study is a combination of aspects that, overall, address the vulnerabilities presented by fighting networks. It primarily utilizes the propositions of the netwar model and incorporates innovations from the CT model. Original aspects presented by the netwar model are augmented in bold by recent innovations and practices to provide an enhanced framework.

	Organization	**Doctrine**	**Operations**	**Info Strategy**
Requirements for Effective Counter-Network Operations	*Decentralized nodes *Lower-level Autonomy *All-channel connections	***Offensive** Swarming ***Illumination** ***Exploitation**	*Synchronized *Decisive Engagements ***Operational Tempo** ***Surprise** ***Fusion** *Pulsing	*Synchronized with Operations *Information diffusion ***Info Disruption** ***Connectivity**

Table 4. An Effective Counter-Network Framework

[380] Spulak and Turnley, "Theoretical Perspectives of Terrorist Enemies as Networks," 26.

The counter-network operations framework is organizationally much closer to a network than any other organizational form. It is characterized by the advantages inherent in increased communication among nodes. Nodes are dispersed to facilitate rapid maneuver and information gathering from a variety of sources, and they enjoy a high degree of autonomy to react to changing local situations. This is not to suggest that it is an organizational form without authority, or any controlling mechanisms, however, authority, and many of the other functions, are not limited to vertical structures. Authority is present in the form of leadership that provides clear guidance and intent, and then facilitates the overall effectiveness of the network. Aspects of control govern the communications infrastructure that facilitates all-channel connections while maintaining its security, and at the same time, pushing for increased communicating nodes.

Doctrinally, the counter-network framework utilizes the primary doctrine of netwar, swarming. Swarming utilizes many small units in a coordinated method that provides the capability to counter the dispersed, highly autonomous actions of fighting networks. Swarming both requires a high degree of information, but also provides it, as individual nodes act as sensors as well. These individual nodes are able to act on this information through a high degree of decentralized C2, to the point where “decontrol” is a more appropriate descriptor than commonly accepted versions of military C2. Swarming may be utilized effectively in a defensive role, but the concealment challenge presented by fighting networks requires an offensive approach. Concealment allows fighting networks the ability to conduct attacks with little indication, and the stealthy nature of their operations requires an offensive approach that places fighting networks on the defensive. When these networks have the freedom to plan and conduct attacks without being pressured, they will succeed at a remarkable rate, against nearly all defensive measures.

Illumination is a prerequisite for swarming, countering the essential concealment of fighting networks. Illumination is a key variable given the overall nature of irregular warfare, and it must be the driving component in a comprehensive approach to countering fighting networks. Illumination provides the understanding to “see” the network, enabling both direct and indirect swarming attacks, as well as the focused and integrated use of

information disruption. Illumination goes beyond traditional intelligence, which is usually a supporting function to a primary operational focus. Illumination ensures that intelligence is not only the main effort in countering networks, but also the driving focus behind all efforts. Exploitation supports the illumination focus and recognizes the importance of understanding the network from the inside out. Instead of providing a secondary means of information, exploitation becomes a primary aspect supporting illumination activities. Exploitation involves both physical, or technical, aspects, as well as the social, or human dimension, and is especially critical in the later. Fighting networks are social networks and understanding the complex and ever-changing, human dynamics requires intimate involvement with members of these networks.

Operationally, much of countering networks stems from the principles presented in the netwar model. Countering networks requires a high degree of synchronization, which is obtained through an emphasis on all-channel connectivity. This synchronization enables fusion, which is a systematic operational method at the center of counter-network efforts. Fusion is about collaboration, and it contains an organizational dimension, as well as a doctrinal dimension. Organizationally, fusion is a product of highly connected elements with the authority and capability to share information constantly and rapidly. Doctrinally, fusion provides a systematic way of melding intelligence efforts with operational efforts to achieve greater degrees of illumination against largely clandestine networks. While especially evident at the operational level, fusion ties together strategic and tactical efforts in ways that are unique to such a system. Fusion provides the capacity for a high operational tempo, which appears to be essential in countering the adaptive flexibility displayed by networks. All of these efforts contribute to surprise, an essential feature most evident at the tactical level, but also a product of innovative strategies.

An effective counter-network framework recognizes that information strategy provides potentially tremendous gains in countering network. Such an information strategy provides operational guidelines and is a pro-active and integral part of both shaping the information environment and conducting decisive information operations. Recognition of the dominant role of information in today’s conflicts provides a guide for all actions against fighting networks. Information disruption flows from this recognition,

and is focused on countering a fighting networks information strategy, including the communications capability it employs. Information disruption seeks to negate, or diminish the overall purpose of a fighting network, as well as interdict, deny, and channel its communication efforts. Information disruption efforts form part of an overall information strategy, and are connected and synchronized within the entire counter-network process.

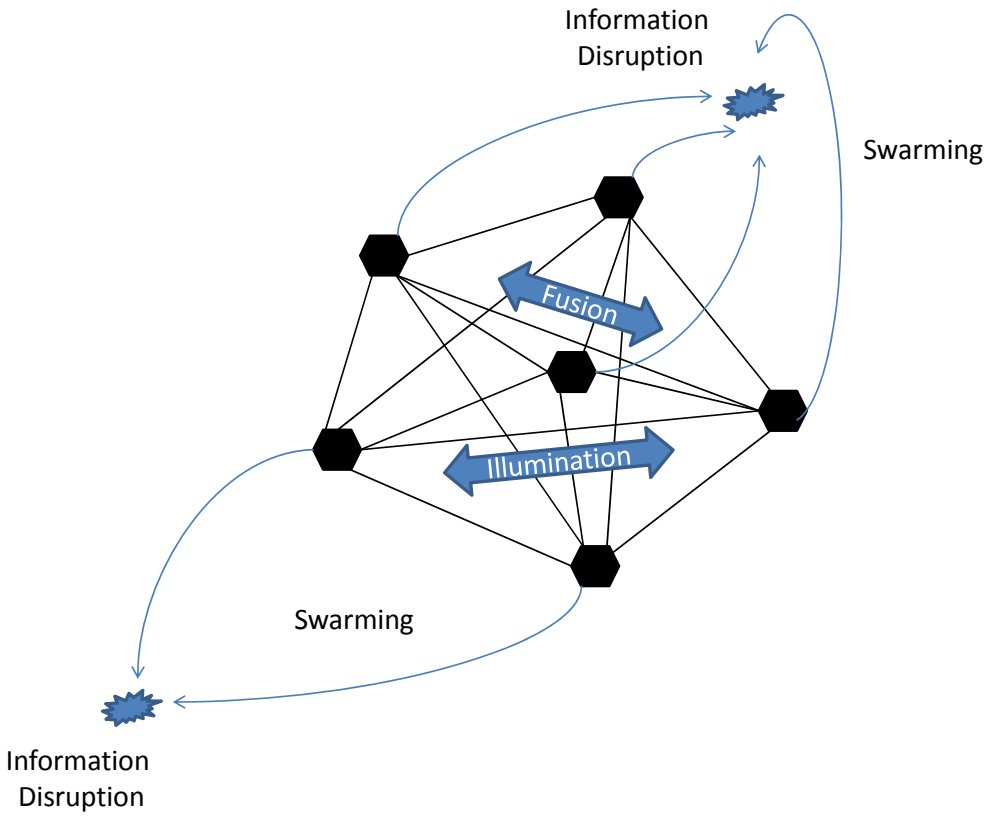

Figure 11. Illustrated Effective Counter-Network Operations

The counter-network framework is composed of variables, which are highly inter-dependent; that is, they require interaction with each other to produce any degree of effectiveness. The framework will be tested for its effectiveness in an examination of fighting networks present in each of the three case studies. Each case study presents several of approaches, as well as combinations, employed over-time, which will provide indicators of the effectiveness of the framework, as well as its applicability to a wide-

range of irregular warfare environments and circumstances. The framework itself provides a model for countering networks, but must be applied in context and is still reliant on coherent strategic application. Forms of warfare are only as effective as the strategic approach employing them, and the people involved, but it is clear that the counter-network framework provides a comprehensive tool for countering networks in irregular warfare. As a U.S. Army SF officer stated in the early days of the fight in Afghanistan, "I think that the bottom line is that any strategy requires agile, adaptive, culturally sensitive forces with the authority to make decisions at the lowest levels in order to stay one step ahead of a cunning, ruthless, and determined enemy."[381] The current challenge posed by fighting networks against nation-states, and also in competition with each other, requires a different approach to war-fighting—one based on an effective counter-network framework.

[381] Stanton, *Horse Soldiers*, 373.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RUSSO-CHECHEN CASE STUDY

> Everywhere there are mountains, everywhere forests, and the Chechens are fierce and tireless fighters.[382]
>
> - Russian Commander Tornau, 1845

> A *kishlak* [village] fires at us and kills someone. I send up a couple planes and there is nothing left of the *kishlak*. After I've burned a couple of *kishlaks* they stop shooting.[383]
>
> - Russian Vice President Alexander Rutskoi

A. CASE STUDY OVERVIEW

The Russo-Chechen conflict provides a vivid example of fighting networks, and the ongoing struggles in that region starkly illustrate the challenges they pose. Chechen irregular warfare is nearly legendary for both its epic nature and brutality, and multiple dimensions are examined in strategic studies on a constant basis. Chechnya's sophisticated irregular warfare, complex population dynamics, and rugged terrain confound simple descriptions, and provide for a rich case study. The seemingly continuous Russo-Chechen struggle reflects the timeless nature of irregular warfare, as well as the dramatic changes in how such warfare is being conducted.[384] Since the end of the 18th century, dozens of Russian military campaigns in Chechnya have been conducted, but the latest series, of the last two decades, is noteworthy as a hallmark of change in warfare.[385] The Chechen separatists have changed over the course of the

---

[382] John Baddeley, *The Russian Conquest of the Caucasus* (London: Longmans Green & Co., 1908), 206.

[383] Carlotta Gall and Thomas de Waal, *Chechnya: Calamity in the Caucasus* (New York: New York University Press, 1998), 97.

[384] Recent studies of the conflict focus on the complexity of the irregular warfare, see for example, Hahn, "The Jihadi Insurgency and the Russian Counterinsurgency in the North Caucasus, 1–39; Mark Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus: The Military Dimension of the Russian-Chechen Conflict," *Europe-Asia Studies* 57, no. 2 (March 2005): 209–290, http://dx.doi.org/10.1080/09668130500051833.

[385] Gall and de Waal, *Chechnya*, 37.

conflict as well, from a majority of primarily secular, nationalists, to radicalized jihadist-inspired terrorists.[386] The changes in warfighting and ideology combine to produce a struggle now primarily visible through its terror attacks.

This case study focuses on the two most recent clashes in the struggle, defining them as the 1st Russo-Chechen War (1994–1996) and the 2nd Russo-Chechen War (1999–present), to understand highly networked irregular threats, and responses to such forms of irregular warfare.[387] In the first portion of the study, a traditional Russian military launched a largely conventional attack into Grozny that suffered devastating blows and ultimately withdrew. The second part of the study focuses on the Russian invasion in 1999, and subsequent efforts, which ultimately succeeded in controlling most of Chechnya. The differences and similarities between the two conflicts reveal changes in military strategy on both sides, as well as each opponent's adaptation to the changes of the information age. Further, examining both conflicts provides significant comparison value, and the brief interlude between the wars allows for an examination of the effective application of lessons learned. In addition, the overall length of the conflict provides for a detailed study to determine the presence of effective counter-network efforts, based on the counter-network framework.

B. CHECHEN OVERVIEW

Chechnya is a relatively small, land-locked part of the Caucasus region in southern Russia. Located between the Black Sea and the Caspian Sea, it is bordered by Dagestan to the north and east, North Ossetia to the northwest, Ingushetia to the west, and

386 The use of the term jihad is used throughout to describe Islamists inspired to conduct violent "holy war" as the main aspect of their struggle. While casting such fighters in a favorable light, by using the term, they prefer to justify their actions; it is the most commonly accepted reference.

387 While the Russo-Chechen conflict is generally described as a "war," in Russia, the phrase a "special operation to reestablish constitutional order and the rule of law," is most common. According to Russian military doctrine, the confrontation is a "military conflict," which is defined wider than overt war and which also includes "armed conflict," a term most closely analogous to the Western concept of "low-intensity conflict" developed in the 1970s. However, while borrowing the concept, the Russians retained much of their own military doctrine, rather than the population-centric focus of LIC and its subsequent refinement as irregular warfare. Since the armed conflict in Chechnya did not require the mobilization of the entire Russian state, it was not considered a war, but for the Chechens, it is just the opposite, and very much a full-scale war. Stasys Knezys and Romanas Sedlickas, *The War in Chechnya* (College Station, TX: Texas A&M University Press, 1999), 1.

the Georgian Republic to the south. The capital, Grozny, is in the centre of the region, located between mostly arid steppes to the north, and a more rugged, mountainous region in the south. The Caucasus Mountains in the south provide a key advantage for Chechens seeking concealment, and to facilitate cross-border movement between Chechnya and the borders of Georgia, Dagestan, and Ingushetia. In many ways, the mountains provide a symbol of Chechnya itself, and the geographic term that refers to the mountainous regions in the country, "Ichkerija," is incorporated into the name of the semi-autonomous region—the Chechen Republic of Ichkerija.[388]

Figure 12. Chechnya and the Northern Caucasus Region[389]

[388] Knezys and Sedlickas, *The War in Chechnya*, 324–330.

[389] University of Texas at Austin, University of Texas Libraries, Perry–Castañeda Library Map Collection, Chechenya (Chechen Republic) Maps, http://www.lib.utexas.edu/maps/chechen.html.

The population prior to the renewal of conflict in the mid-1990s was approximately 1.05 million, but it has shrunk to half those numbers due to wartime deaths, resettlement, and displacement throughout Russia and abroad.[390] Among the Autonomous Republics of the Russian Federation, Chechnya was one of only three whose indigenous population constituted the majority, but even in 1994, nearly 30 percent of the population was Russian.[391] Clan and familial organization continues to define much of Chechen society, and its structure provides a fundamental aspect in both Chechen political organization and military action. The Chechen clan is called a *teip*, and it is generally composed of 2–3 villages, with up to 600 people per village, with the capability of producing up to 600 fighters. Within each *teip*, there are sub-clans called *ne'ke* or *gar*, which consist of 10–15 families. *Teips* have a council of elders and provide community policies, regulations, and rulings on economic interests. A total of 150 *teips* exist in Chechnya, with numerous interactive alliances and feuds.[392] *Teips* are grouped into larger tribes called *tukhum*, which are spread across Chechnya and generally grouped by location in either the plains or mountains.[393] This clan-based society provides significant cohesion and connectivity, highlighting the importance of cultural forms in generating fighting networks, "Chechen social networks form the basis for their military organizational structure, imbuing the later with much flexibility and the sort of durability under stress that has been required in the war with the Russians."[394] The clan structure is buttressed by a conservative form of Islam, Sufism, which is traditionally organized into tight societies, adding another layer to the deep connectivity inherent in Chechen networks. Yet, despite such connections, deep divisions, differences, and feuding between various clans also occur. Internal Chechen power struggles are legendary and are largely formed by infighting between mountain and flatland clans.

---

[390] Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 210.

[391] Knezys and Sedlickas, *The War in Chechnya*, 1.

[392] Theodore Karasik, "Chechen Clan Tactics and Russian Warfare," March 15, 2000, 1, http://www.cacianalyst.org/?q=353.

[393] Arquilla and Karasik, "Chechnya: A Glimpse of Future Conflict?" 210.

[394] Karasik, "Chechen Clan Tactics and Russian Warfare," 2.

The struggle for control and autonomy in Chechnya defines much of Russian history, and the region has largely been shaped by a clash of cultures from the Ottoman, Persian, and Russian empires. By the early 18th century, the Russian Empire was exerting consistent influence to control and even subdue the Chechen region.[395] The Chechen response, led by the Circassian leader Ushurma, who adopted the title of Sheik Mansur, provided the beginnings of a modern legacy for autonomy, defined by militant resistance and a fiercely independent political organization.[396] Sheikh Mansur's armed resistance in 1785 united the Circassian population in a call for a holy war against the Russians and managed an initially impressive showing that surrounded and killed 600 Russian soldiers.[397] Although this resistance was effectively over when Mansur was captured in 1791, he provided a model of unified resistance for the North Caucasus.[398] Mansur's historic successor, Imam Shamil, rose to prominence in the Russo-Turkish Wars, and also used Islam to aid in uniting against Russian resistance. Shamil's rebellion began in Dagestan in 1834, but quickly spread to Chechnya, where it was ardently supported.[399] This support led to the development of a rudimentary Islamic state comprised of Chechens, Ingush, and Dagestanis, but Shamil's repressive rule led to an inability to unite the Circassians fully, and the Russians finally defeated him in 1859.[400] However, a desire for independence grew in response to increasing Russian control, and "a significant portion of the population rallied to rebel leadership as each generation brought a new burst of resistance to Russian domination, most often led by men of religious status."[401]

---

[395] The Circassian term describes the Caucasian people living in the Western Caucasus, although ethnographic opinions differ throughout history, largely due to Soviet attempts to unify the Caucasus region. Paul B. Henze, *The North Caucusus: Russia's Long Struggle to Subdue the Circassians* (Santa Monica: RAND, 1990), 16.

[396] Gall and de Waal, *Chechnya*, 38.

[397] Ibid.

[398] Paul B. Henze, *Russia and the Caucasus* (Santa Monica, CA: RAND, 1996), 7.

[399] Gall and de Waal, *Chechnya*, 39.

[400] Paul B. Henze, *Islam in the North Caucasus* (Santa Monica: CA, RAND, 1995), 12.

[401] Ibid.

Following in the tradition of Sheikh Mansur and Imam Shamil, the next resistance leader, Sheikh Najmuddin, saw the Bolshevik Revolution as an opportunity to rise up, and in August 1917, he was elected Imam of Dagestan and Chechnya.[402] This attempt at autonomy was again fiercely repressed, starting a cycle that featured alternating accommodation and revolt against Bolshevik control, culminating in 1937 with Stalin's arrest and execution of over 14,000 Chechen and Ingush.[403] WWII provided another opportunity for rebellion, which was again crushed by vicious repression and a deportation intended to liquidate Chechnya and Ingushetia. In 1956, Khrushchev lifted the exile, resulting in a flood of Chechens back into the region.[404] Order was again imposed by Soviet troops, which led to a fairly long period of relatively low-scale clashes and unrest up until the fall of the Soviet Union in 1991.

In 1991, a Chechen government, under former Soviet Air Force General Dzhokar Dudayev, sensed weakness during the changes occurring in the Soviet Union, and declared independence. As Chechen's newly independent government sought increasing control, opposition groups, which favored remaining as a part of the Russian Federation, formed against Dudayev. These groups, backed by Russian military and intelligence agency assistance, initiated a series of smaller clashes, even as the Russian Army withdrew from Chechnya.[405]

C. THE 1ST RUSSO-CHECHEN WAR: 1994–1996

The 1st Russo-Chechen War had its origins in Dudayev's declaration of independence in the wake of the 1991 Boris Yeltsin inspired autonomy movement, but it would take several years before it flared into a large, open conflict.[406] As the newly formed Chechen government, the independent Chechen Republic of Ichkerija (ChRI), began to acquire former Soviet military equipment and arm itself, which was met by

[402] Henze, *Russia and the Caucasus*, 3.

[403] Gall and de Waal, *Chechnya*, 53.

[404] Aleksander M. Nekrich, *The Punished Peoples*, trans. George Saunders (New York: W.W. Norton and Co., 1978), 147.

[405] Knezys and Sedlickas, *The War in Chechnya*, 23–32.

[406] Finch, "Why the Russian Military Failed in Chechnya," 1.

clandestine Russian efforts to back Chechen opposition groups. However, these Russian attempts at gradually backing the opposition movement, to include providing tanks and crews, were soon made public. In addition, their Chechen proxies were making little progress, and were significantly repulsed in an effort to seize Grozny on November 29, 1994.[407] President Yeltsin made the decision to deploy regular Russian forces openly, and on December 11, 1994, the Russians entered Chechnya.[408] The initial invasion of Chechnya was a primarily conventional affair with Russian forces numbering nearly 40,000, intent on dominating the insurgent Chechen forces of around 1,000 with superior mass and firepower.[409] The most notable incident during the initial invasion was the fate of a Russian armored column spearhead that drove into the capital of Grozny. This spearhead was met with a withering counter-attack composed of decentralized and autonomous units operating in small teams, which inflicted huge casualties. Then Colonel Alan Maskhadov, whose leadership provided a unique vision of warfare, and who was promoted for his success, spearheaded the defense of Grozny.[410] Ultimately, the Russians reinforced their initial elements and succeeded in taking Grozny in February 1995 when the last Chechen units withdrew from the city. The Chechens were never beaten on a tactical level, choosing to withdraw when Russian forces advanced south and initiated their cordon and bombardment of any defended villages or towns.

The second phase of the war was marked by rural engagements to the east, west, and south of Grozny, and was notable for aerial and artillery bombardment against villages, resulting in the killing of thousands of civilians.[411] By mid-June, 1995 Russian forces had penetrated through the mountains to some of the most southern villages, and

---

[407] This significant effort was actually the first assault of Grozny and its outcome would foreshadow the initial Russian attempts at taking the city. The opposition groups were secretly reinforced with Russian tanks and airpower, of which Chechen fighters reported 32 tanks and five armored vehicles destroyed, 12 captured, and four helicopters shot down. Despite the outcome, Russian forces would employ the same approach, with far greater consequences, during their overt invasion a month later. Knezys and Sedlickas, *The War in Chechnya*, 46–51.

[408] Finch, "Why the Russian Military Failed in Chechnya," 2.

[409] Gall and de Waal, *Chechnya*, 188.

[410] Knezys and Sedlickas, *The War in Chechnya*, 107.

[411] Arquilla and Karasik, "Chechnya: A Glimpse of Future Conflict?," 211.

had declared the campaign a success.[412] However, during the same month, one of the Chechen commanders, Shamil Basayev, infiltrated into Russia using Russian army uniforms and equipment and raided the town of Budinovsk and took over 1,500 hostages. After repulsing multiple attempts by the elite *Alfa* special operations unit, the Chechens were allowed to return to Chechnya under the protection of a ceasefire.[413] While condemned for its terror, this raid on Budinovsk forced Russia to initiate negotiations and a brief ceasefire, which is a significant outcome for a "…military-diversion operation conducted by, at best, a company of soldiers…," and it "…succeeded in stopping a vastly more powerful country's savage war of annihilation…."[414] The Budinovsk raid was a strategic counter-attack that forced the Russians to re-evaluate their position, and combined with heavy combat losses on both sides, led to a series of short-lived negotiations. A second significant raid occurred in January 1996, when another Chechen unit, under the command of Salman Raduyev, penetrated into Russia and took over 3,000 hostages in the town of Kizlyar. During its withdrawal, with hostages loaded on buses, it was stopped in the Russian town of Pervomaiskoya and was besieged by elite forces, including *Alfa*. The assaults lasted over three days, but the Russians were continuously repulsed, and eventually, they pulled back and bombarded the town with heavy artillery. The Chechen fighters managed to slip out through the Russian positions during the bombardment, and the devastation and loss of life resulting from these raids resulted in significant media attention and public condemnation.[415] In a rather bleak period of diminishing Russian gains, they scored a success with the successful targeting of Dudayev, finally triangulating the position of his satellite telephone and launching aircraft-fired rockets against his vehicle on April 21, 1996.[416]

---

[412] Robert M. Cassidy, *Russia in Afghanistan and Chechnya: Military Strategic Culture and the Paradoxes of Asymmetric Conflict* (Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 2003), 45, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB125.pdf.

[413] Dimitri V. Trenin and Aleksei V. Malashenko, *Russia's Relentless Frontier: The Chechnya Factor in Post-Soviet Russia* (Washington, DC: Carnegie Endowment for International Peace, 2008), 23–24.

[414] Knezys and Sedlickas, *The War in Chechnya*, 173.

[415] Cassidy, *Russia in Afghanistan and Chechnya: Military Strategic Culture and the Paradoxes of Asymmetric Conflict*, 46.

[416] Knezys and Sedlickas, *The War in Chechnya*, 311–313.

Regaining the initiative, Chechen forces returned to Grozny in August 1996, in a well-planned operation led by General Maskhadov, which served as a gesture of defiance on Yeltsin's inauguration day.[417] Dressed as pro-Moscow militiamen, numerous small nodes infiltrated the city, bypassing Russian static checkpoints and guard posts largely unoccupied at night, and bribing others that were actually manned.[418] Early on the morning of the 6th, over 5,000 Chechen fighters, led by Shamil Basayev, attacked individual Russian strongpoints while other fighters set up ambush positions along all possible reinforcement routes. The Chechen forces took the majority of the city and pushed Russian forces back to pre-assault positions held in 1994, and in one day, Russian casualties amounted to 500 dead and 1,500 wounded.[419] The Russian counter-attack was primarily a stand-off affair, using artillery, tanks, and aerial bombardment from outside the city, but two relief columns attempted to penetrate the city. These armored forces were repulsed with vicious swarming attacks much like those that plagued the initial drive into Grozny less than two years prior. The Russians realized that any attempt to "liberate" Grozny would require massive devastation, and most likely, the loss of thousands of surrounded Ministry of Internal Affairs (MVD) forces, and by the end of August, the Khasavyurt peace accords were signed. Russian troops withdrew from Chechnya and establishing a five-year ceasefire.[420]

The 1st Russo-Chechen war, forecast to last just days, developed into a full-scale, but highly irregular war against Russian forces. According to the Russian official estimates, 3,826 soldiers were killed and 17,892 were wounded, with over 1,900 missing, but other accounts place the Russian losses at least twice as high.[421] The Chechen fighting network combined clan-organization, Russian army experience, and an influx of a number of Afghan jihadists as "'consultants' to teach Chechens how to fight using the

---

[417] Knezys and Sedlickas, *The War in Chechnya*, 258.

[418] Robert Seely, *Russo-Chechen Conflict 1800–2000: A Deadly Embrace* (London: Frank Cass, 2001), 272.

[419] Cassidy, *Russia in Afghanistan and Chechnya: Military Strategic Culture and the Paradoxes of Asymmetric Conflict*, 47.

[420] Seely, *Russo-Chechen Conflict 1800–2000*, 289.

[421] Gall and de Waal, *Chechnya*, 399.

same guerrilla tactics that proved so successful against Soviet forces in Afghanistan in the 1980s."[422] The Chechen forces incorporated these tactics into their network-style warfare, which was made possible by their clan structure and modern communications, and fielded highly capable nodes synchronized into an impressive fighting network. The 21-month conflict went from being forecast as a "'bloodless blitzkrieg'' to a full-scale defeat of an ill-prepared and almost entirely conventional army, and provides a stark example of a traditional army attempting to fight irregular and highly networked unconventional opponents.[423] The notable brutality of the war was shocking to participants, especially outside observers expecting a "low-intensity conflict." The overwhelming Russian repression and destruction they inflicted on the Chechen civilians bordered on extermination, and was met by Chechen terror attacks and executions of Russian soldiers.[424]

The Chechen's are generally considered to have won an overwhelming victory against a superior force. The Chechen military commander and future president General Maskhadov's self-described "semi-guerrilla war," notable for its swarming tactics and decisive battles, illustrated just how challenging a robust network of irregular opponents could be.[425] Despite initially aiming to develop a conventional army, to demonstrate Chechnya's capabilities and reinforce its independent stature, Maskhadov quickly realized that a new strategy would pay far greater dividends, and encouraged his military forces to disperse into very capable semi-autonomous units. The Chechen fighting networks continued to learn throughout the war, and six months after they had withdrawn from Grozny, they were re-established through the countryside and controlled nearly all territory the Russians did not physically occupy. While the Khasavyurt accord specified a

[422] Murphy, *The Wolves of Islam*, 19.

[423] Finch, "Why the Russian Military Failed in Chechnya," 4.

[424] Knezys and Sedlickas, *The War in Chechnya*, 321–322.

[425] Gall and de Waal, *Chechnya*, 313.

five-year ceasefire, and the resolution of the final status of Chechnya by the end of 2001, these negotiations never occurred due to incursions by Chechen Islamists into Dagestan in August 1999, which initiated the second phase of the conflict.[426]

1. Russian Invasion

The Russian invasion into Chechnya followed the traditional Russian doctrine of a deep penetration attack to seize key terrain. It appears that the Russian inner circle believed, despite having failed in multiple coup attempts, that the full invasion would be a walkover. The Russian Minister of Defense General Pavel Grachev is said to have thought that one paratroop regiment would be able to conquer Chechnya in just two hours.[427] By massing their large army, the Russian high command felt that they would be able to overrun the "band of criminals" swiftly.[428] Russian soldiers were told that they would swiftly dispatch the untrained and unorganized Chechen forces, and that the sight of Russian tanks would force the rebels to back down. However, having previously relied on extensive clandestine efforts to unseat Dudayev, the detailed planning for a large traditional military operation did not begin until just two weeks prior to the invasion.[429] This haste reflected the confidence the Russians had in their much larger and better equipped conventional forces.

Organizationally, the Russian forces were based on a traditional model, the former Soviet army, but their performance demonstrated how unsuited the Russian military actually was for fighting a network. "It also demonstrated how poorly Russian military organizational structures functioned when disparate forces were called to work together."[430] The force that was pulled together to invade Chechnya was assembled

---

[426] Mark Kramer, "The Perils of Counterinsurgency: Russia's War in Chechnya," *International Security* 29, no. 3 (Winter 2004/2005): 5, http://belfercenter.ksg.harvard.edu./files/kramer.pdf.

[427] Stephen J. Blank and Earl H. Tilford, *Russia's Invasion of Chechnya: A Preliminary Assessment* (Carlise Barracks, PA: U.S. Army War College Strategic Studies Institute, 1995), 13.

[428] Ibid.

[429] Finch, "Why the Russian Military Failed in Chechnya," 2.

[430] Olga Oliker, *Russia's Chechen Wars 1994–2000: Lessons Learned from Urban Combat* (Santa Monica, CA: RAND, 2001), x.

hastily and demonstrated a dramatic lack of coordination, with no combined training.[431] A number of different ministries and organizations deployed troops to Chechnya, but each in their own separate command structures leading to a confusing command structure and considerable in fighting over roles. Overall, coordination between the Ministry of Defense (MoD) and MVD units was nearly non-existent.[432] These bureaucratic "stovepipes" extended all the way down to the lowest tactical levels, and included each respective organization's air and ground forces. Some analysts cite this as the "single, over-riding cause behind the Russian defeat in Chechnya," and highlight a lack of unity of command, "it is not only the lack of cooperation between the troops of the ministry of defence, the ministry of internal affairs and the federal security bureau, which could have been predicted. It is also the backbiting between units and senior commanders in the army which is so alarming."[433] Overall, the Russians were organized in classic, hierarchical fashion and this continuation of the centralized, bureaucratic nature of Soviet military structure proved ill-suited for complex irregular warfare in Chechnya.

Following the Russian failure during the initial assault on Grozny, more experienced forces, primarily special operations, began arriving alongside thousands more MVD forces. These special operations elements were composed of naval, infantry, and *speztnaz* fighting units, and were smaller than the conventional forces they replaced.[434] This smaller size, combined with greater capabilities and a much higher degree of autonomy, produced a greater agility. However, they faced dramatic challenges from their own disunity of command, and were not employed as effectively as possible due to Russian doctrinal issues. Reserved primarily as "shock-troops" against concentrations of Chechen forces, they rarely succeeded in inflicting serious loses, and found themselves occupying terrain more than pursuing Chechen cells.

Doctrinally, the Russian forces that entered Chechnya were products of Soviet doctrine, and had, "…focused almost exclusively on war in central Europe against a

---

[431] Oliker, *Russia's Chechen Wars 1994–2000*, x.

[432] Ibid., xi.

[433] Finch, "Why the Russian Military Failed in Chechnya," 10.

[434] Knezys and Sedlickas, *The War in Chechnya*, 110.

highly skilled, technologically advanced adversary."[435] This doctrine assumed that fighting in Central and Western Europe would present cities either defended, or left wide open in the hopes they would not be destroyed by combat. Defended cities were to be bypassed, while open cities would be entered in a massive show of force led with tanks and following with mounted infantry. Despite a deep legacy of urban combat and experience in WWII, by the 1980s, the MoD largely ignored urban combat.[436] Instead, it focused on a concept of massed forces conducting large-scale maneuver, but often applying a linear approach to seize territory. However, for this kind of warfare to be successful, even against a similar opponent, a great degree of synchronization must occur, and it must be supported by a responsive logistical system .[437] The Russians failed to deliver either, and instead, produced uncoordinated efforts whose most notable doctrinal effect was large-scale indiscriminate indirect fires. Nearly a year into the conflict, Russian forces did strive to update their doctrine and develop better small-unit tactics, but these had mixed results because their overall doctrinal approach still sought to avoid direct small-unit combat and rely more on air and artillery bombardment. This heavy repression led to the merciless destruction of numerous Chechen villages, and it is likely "…that some of the worst wartime atrocities inflicted in the last half century occurred in Chechnya."[438] It may be that the only true signs of unconventional activity by the Russian military were the use of "disruption-diversion" groups, which conducted abductions, kidnappings, and killings to accomplish political goals and promote a sense of overall lawlessness under the assumption that this would drive a desire for Russian control.[439]

This doctrinal approach was compounded by errors in operational methods. Most notable was a lack of intelligence preparation and reconnaissance in advance of their

---

[435] Oliker, *Russia's Chechen Wars 1994–-2000*, 2.

[436] This was true of many of the world's professional militaries at the time, and it was only after the events in Mogadishu in 1993, and Russia's brutal experience in 1994, that the United States began focusing more on urban combat. Oliker, *Russia's Chechen Wars 1994–2000*, 2.

[437] Finch, "Why the Russian Military Failed in Chechnya," 8.

[438] Knezys and Sedlickas, *The War in Chechnya*, 320.

[439] Ibid., 322–323.

efforts. “Because communications procedures and equipment were often incompatible, intelligence frequently could not be shared, and units were unable to transmit their locations to supporting air forces.”[440] Moreover, the three different invasion groups that crossed the border were unsynchronized, which resulted in significant delays and a lack of surprise.[441] Tactically, the Russian forces were simply unprepared for irregular warfare; they lacked the requisite small-unit skills and were especially deficient in urban combat training. The initial Russian assault on Grozny in 1994 was an attempt to take the city on the march by using tanks and armored personnel carriers (APCs) in maneuver columns. This operation followed their doctrinal assumptions, but the lack of infantry allowed the Chechens to funnel Russian forces into complex ambushes, where they were decimated in well-prepared kill zones.[442] A notable contributing factor was the overall inexperience and lack of training of Russian forces, many of whom were conscripts believing they would be fighting a short war. The deployment of better-trained soldiers, naval infantry and other elite units, served to increase the overall capability, but on the whole, the Russian operations proved largely inefficient.

The Russians had little to no information strategy in during their 1994 invasion and even through their eventual withdrawal in 1996. According to Stephen Blank and Earl Tilford, the Russian command was nearly oblivious to the emerging effects of a war waged in the information age, and failed to account for numerous factors:

> Nor did the planners count on the reluctance of commanders to fire on unarmed civilians or on the corrosive effects on the military of official lying during Russia’s first ‘television war’. Free broadcasting from the war zone belied the hollow claims made about a lack of Russian or civilian casualties and brought into question the reasons for the war. Nor did Russian audiences enjoy seeing their forces engage in the terror bombing that ensued when the ground forces failed to advance over land.[443]

---

[440] Oliker, *Russia’s Chechen Wars 1994–2000*, 14.

[441] Gall and de Waal, *Chechnya: Calamity in the Caucasus*, 172.

[442] Lester Grau, “Changing Russian Urban Tactics: The Aftermath of the Battle of Grozny,” http://www.globalsecurity.org/military/library/report/1995/grozny.htm, first published in *INSS Strategic Forum* 38, July 1995.

[443] Blank and Tilford, *Russia’s Invasion of Chechnya: A Preliminary Assessment*,” 13.

Russian forces did attempt to conduct information operations, but this was primarily seen in basic psychological warfare, with the use of leaflets, loudspeakers, and electronic broadcasts. In many cases, the message, that Russian operations were to disarm illegal Chechen "bandits," sent by Russian propaganda served actually to lull the Russian soldiers into a sense of complacency about the true nature of the fighting they would face. When received on the Chechen side, these and similar messages provoked Chechen resistance by emphasizing treason and promoting Grachev's orders to deport Chechens.[444]

2. Chechen Network Response

The Chechen response to the Russian invasion produced a unique display of irregular warfare. The Chechens fought based on a strong background of military experience and within the framework of a socially decentralized society. Ironically, the Russian army trained many Chechen fighters, and their participation in conflicts occurring in the emerging Trans-Caucasian states from 1991–1994 provided significant experience for elements like Basayev's Chechen Battalion. This unit fought in the Abkhazian succession movement, was trained by Russian Military Intelligence (GRU) and *spetznaz* forces, and would go on to be one of the more formidable groups in the Russo-Chechen conflict.[445] The unconventional tactics Chechen networks displayed utilized a few aspects of guerrilla warfare, but reflected a paradigm shift. Maskhadov receives most of the credit for this approach, recognizing the unique combination of training, connectivity, and "home-field advantage" his forces enjoyed. Encouraging considerable autonomy, he promoted high degrees of self-organization and innovation through the force. Instead of using just hit-and-run tactics, Chechen fighters aggressively attacked Russian elements, with the goal of destroying whole units. Instead of withdrawing, small bands of fighters continuously maneuvered against Russian forces from multiple directions and displayed a remarkable staying power and penchant for

444 Knezys and Sedlickas, *The War in Chechnya*, 85.

445 John B. Dunlop, *Russia Confronts Chechnya: Roots of a Separatist Conflict* (London: Cambridge University Press, 1998), 145.

close-in fighting. Chechen fighting networks combined modern information technology with a cohesive social network that enabled small, autonomous, swarming units, which provided a clear example of dramatic changes in irregular warfare.

Organizationally, the Chechen forces were largely an ad hoc network that had little hierarchical structure. Despite having a senior command, at the operational and tactical levels, the Chechen forces were extremely "flat" consisting of numerous smaller units, or nodes, of "non-standard squads." In their excellent study of the assault on Grozny, Stasys Knesys and Romanas Sedlickas described Chechen forces:

> During the repulsion of the assault, the Chechen forces operated almost independently. Many small groups of Chechen fighters in the city also found themselves appropriate places in the city's defenses. Everyone's basic purpose was, after all, the same: to destroy the enemy. These mobile, completely independent groups chose their targets themselves and, being always on the move, created for the Russian units the appearance of a unified attack. The coordination among the leaders of the Chechen fighter groups was, however, exceptional. Even without centralized command, they succeeded in fighting their opponent all over the city simultaneously.[446]

Each element was comprised of heavily armed personnel with a mix of weapons and communications equipment, producing highly capable, but still extremely agile teams. These teams formed "hunter-killer" groups of fighters, possibly represented by two men with RPG-7 or RPG-18 anti-tank grenade launchers, two with medium machine guns, several riflemen, and a sniper. Multiple teams formed a cell, with additional support elements, such as medical, ammunition bearers, or additional snipers. Three cells composed a larger element of 75–100 men, which included a mortar crew and command and planning cell.[447] This networked organization built on the clan-based social networks that play such a significant role throughout Chechen society. William Nemeth highlights several points drawn from descriptions of Chechen organization, including the fact that *teip* members rotate in and out of battle, the overall number of fighters can be quickly expanded through supporting groups, that the fighters are physically supported by a dense

[446] Knezys and Sedlickas, *The War in Chechnya*, 107.

[447] Oliker, *Russia's Chechen Wars 1994–2000*, 19.

"…network of kinship and religious relationships while engaged in fighting…," and that this flexible organization allows rapid re-organization between smaller-decentralized operations and larger synchronized efforts.[448] According to both Russian and Chechen accounts, Chechen organization was both simple and fluid, but highly effective. It allowed dispersed semi-autonomous units to swarm in self-coordinated raids, but also to re-consolidate for larger, more complex operations.

Doctrinally, the Chechen forces made extensive use of rugged natural terrain and incorporated the hard-learned urban combat lessons of the Soviet era. They sought to maximize the asymmetry in force with a doctrine of swarming that culminated in aggressive close-in fighting. The overall outcome of the war was largely shaped by the Chechens' "…exploitation of the network form of organization and a related capacity for swarming attacks."[449] This exploitation allowed the Chechen teams to converge against exposed Russian forces to attack, and then rapidly redisperse once destroyed. These Chechen units provided an ideal fit for swarming, which "…will work best—perhaps it will only work—if it is designed mainly around the deployments of myriad, small, dispersed, networked maneuver units."[450] Complimenting this doctrine, was highly unorthodox techniques, such as arming small cells with heavy weaponry, for instance arming a unit of 10–20 men with 12 grenade launchers, when "as a rule, a group of ten men had only one grenade-launcher."[451] The swarming displayed by Chechen forces in the defense of Grozny, as well as in multiple other significant engagements, highlights the differences in doctrine from traditional guerrilla war. The Chechens neither relied on traditional guerrilla hit-and-run attacks nor sought to develop larger conventional forces, as Mao theorized. Instead, using small bands of fighters, they demonstrated the ability to seize the initiative continuously and decisively defeat larger, better-armed forces. Rather

---

[448] William J. Nemeth, "Future War and Chechnya: A Case for Hybrid Warfare" (Master's thesis, Monterey, CA: Naval Postgraduate School, 2002), 54.

[449] Arquilla and Karasik, "Chechnya: A Glimpse of Future Conflict?," 212.

[450] John Arquilla and David Ronfeldt, "Networks, Netwars, and the Fight for the Future," 16, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/889/798.

[451] COL Husein Iskhanov, Interview from June 1999, *Small Wars Journal*, 6, www.smallwarsjournal.com.

than hasty attacks and withdrawals, Chechen swarming attacks sought to deliver punishing blows, and on numerous occasions, destroyed complete Russian elements.[452]

The operational methods utilized by the Chechens highlight their unique use of unconventional tactics, perhaps the most significant display of irregular warfare in the modern era. Their small-unit organizing principles were ideal for urban terrain and were well suited for the close-in fighting required. Chechen fighting networks utilized unconventional tactics based on a deep understanding of urban combat, and displayed the operational agility to swarm in concentrated attacks, while still being able to disperse rapidly. Chechen hunter-killer teams perfected the art of close in ambushes, stealthfully infiltrating as close as possible to Russian forces. Their willingness to utilize all forms of concealment provided a significant advantage, and largely negated the Russian emphasis on stand-off weapons. The tactics they displayed illustrate the swarming doctrine and emphasize the potential for small, but well-connected forces confronting larger, massive formations. These tactics were clear in the Chechen employment of rocket-propelled grenade (RPG) teams, which swarmed to destroy sixty62 tanks in the first month of fighting, and stealthy sniper teams. Effective employment of snipers proved devastating, as in one Russian battalion, only one officer and 10 soldiers survived sniper fire.[453] The sniper teams also successfully attritted and slowed the Russian formations, which forced them to deploy indirect firepower, and made them more vulnerable to swarming RPG teams. Once they made contact with Russian forces, snipers and machine gun teams would establish a hasty ambush, while anti-armor teams move in close for precision kills. "The teams deployed at ground level, and also in second and third stories and in basements. Normally, five or six hunter-killer teams attacked an armored vehicle in unison. Kill shots were generally made, as noted above, against the top, rear, and sides of vehicles."[454] Moreover, the Chechens had access to Russian communications, "…which in the early days of conflict were transmitted in the clear, in large part because the forces operating the equipment were not familiar with the necessary procedures for secure

[452] Knezys and Sedlickas, *The War in Chechnya*, 77.

[453] Ibid., 106.

[454] Arquilla and Karasik, "Chechnya: A Glimpse of Future Conflict?," 214.

communications."[455] In addition, Chechen forces had access to both Russian radios, as well as their own commercial Motorolas, providing them with the capability to monitor Russian communications on their own military radios, while still having their own secure means.

> We had a special room in the Palace [Presidential Palace in Grozny] for radio operators. Whenever we had a moment, we would go there to 'talk' to the Russians. We listened to their call-up, waited for the moment when they were giving orders having determined who was in command and who was a subordinate. Then we intervened, giving different orders in a confident manner, providing false positions, and so on. As a result, the Russians suffered more losses at the beginning of the war through friendly fire than through our efforts.[456]

The fact that most Russian did not speak Chechen ensured that the Chechen units could enjoy secure communications simply by speaking in their native tongue.[457] This simple difference provided a fundamental advantage for Chechen forces, one that greatly enhanced their ability to both disrupt Russian communications and retain the flexibility of speaking freely. In addition to collection on Russian communications, Chechen commanders also utilized extensive intelligence networks, gathered by the local population and special reconnaissance teams.[458]

Chechen information strategy derived significant strength from a cohesive narrative—one based on the idea of a free and proud Chechnya. This powerful "story" is clearly present in the following sections of the Chechen national anthem:

> Our mothers dedicated up to our Nation and our Homeland.
> And we shall all rise up to the last one if our nation needs us.
> We grew up free as the eagles, princes of the mountains.
> There is no threshold from which we shall shy away…..
> Never to bow our heads to anyone, we give our sacred pledge.
> To die or to live in freedom is our fate….

---

[455] Oliker, *Russia's Chechen Wars 1994–2000*, 18.

[456] Iskhanov, Interview from June 1999, 4.

[457] Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 250.

[458] Knezys and Sedlickas, *The War in Chechnya*, 78.

> If we shall be forced to starve from famine, we shall gnaw the roots of trees.
>
> If we shall be deprived of water, we shall drink the dew from the grass.
>
> We came onto this earth when the wolf cubs began to whine under the she-wolf's feet.
>
> We pledge our lives to God, or Nation and our Homeland.[459]

Building on the theme of a free, but oppressed people, the Chechens consistently emphasized Russia as an aggressor and highlighted the brutality of Russian tactics. The Chechen use of media demonstrated a savvy information strategy that effectively swayed global public opinion. A large number of journalists were present for the conflict and the Chechens deliberately granted access and took steps to influence public opinion. Journalist were provided with open access and encouraged to describe the horrors inflicted against Chechen civilians. Further, demonstrating a savvy appreciation for globalized networks, Chechen officials enlisted support from nongovernmental organizations (NGOs), which "…brought pressure to bear on Yeltsin from outside Russia, while at the same time reaching the Russian mass public, damaging morale, and seriously affecting Russian popular support for the war."[460] This element of their information strategy displayed many of the core characteristics of the netwar concept. Chechen forces also took direct methods to combat Russian information flow at the tactical level and blocked and disrupted communications with captured radios. Further, they also used radio-jamming equipment to block Russian mass media within Chechnya, and overrode Russian efforts with their own mobile television platforms.[461]

---

[459] Romanas Sedlickas, trans., as quoted in Knezys and Sedlickas, *The War in Chechnya*, 1.

[460] Arquilla and Karasik, "Chechnya: A Glimpse of Future Conflict?" 217.

[461] Ibid.

1st Russo-Chechen War				
	Organization	Doctrine	Operations	Information Strategy
Russian Forces	*Traditional, Bureaucratic. *Little Coordination *Poor Cohesion	*Deep Maneuver *Overwhelming Force *Seize Key Terrain	*Firepower *Lack of Small Unit Tactics	*Basic Propaganda *Enemy Focused
Chechen Forces	*Decentralized *Numerous small cells *Highly connected	*Swarming *Decisive Operations	*Synchronized Attacks *Capable Small Unit Tactics *Secure Communications	*Powerful narrative *Global audience *Disrupted Russian efforts

Table 5. Evaluation of the 1st Russo-Chechen War

3. Analysis of Counter-Network Framework

Overall, the results of the 1st Russo-Chechen War leave little doubt that the Russian forces failed to achieve any significant aspects of effective counter-network operations. The primary strategy in the launching of their conventional military campaign was to seize key terrain rapidly and force a capitulation from the ChRI. Russia's overall military organization and doctrine was inconsistent with the counter-network theory proposed earlier in this study, and Russian forces never demonstrated any significant portion of the four primary counter-network variables. A report released in 1995 criticized nearly every aspect of Russian military preparations during the initial efforts, which provided clear evidence that Russian capabilities were ill-suited to the conflict they faced.[462]

a. Offensive Swarming

The Russians employed a doctrine that seemed to run counter to the basic elements contributing to effective swarming—operational tempo, surprise, and pulsing.

[462] Knezys and Sedlickas, *The War in Chechnya*, 83–85.

Overall, their forces maneuvered in a fairly linear fashion seeking to "push" Chechen fighters out of key urban areas. Despite improvements and adaptations in small-unit tactics and organizing in smaller, combined battle groups with more infantry and elite unit support, they failed to achieve any of the three aspects of swarming.

The Russian forces failed to achieve any kind of meaningful operational tempo because they were disjointed and lacked coordination, and immediately reverted to stand-off attacks with heavy artillery and weapons when confronted by Chechen forces. While the Russian's slight improvements following their initial entry in 1994 allowed them to take Grozny after hard fighting, "…the level of military effectiveness that they could hope to reach was limited by the Army's organizational structures. Command of even small tactical actions remained centrally controlled, to the point of imposing constraints on the ability of field units to talk to each other."[463] Their response to Chechen raids and ambushes was to withdraw and engage from afar, or if they were static, to remain in secure defensive positions. While later improvements and more specialized units brought small unit resoluteness and audacity to bear, overall, the Russians lacked the tactical mobility to sustain any significant operational tempo. Chechen fighters countered their reliance on helicopter infiltration with mobile anti-aircraft teams that would attack targets of opportunity, but also swarm to landing zones as the Russians attempted to insert.[464]

The start of the invasion demonstrated the Russians' inability to achieve significant surprise. Except for aerial bombardment, Chechen forces were rarely caught by surprise, and seemed to know nearly every Russian plan. Tactically, Chechen units retained the initiative in nearly every engagement, luring both armored columns and helicopter assets into pre-arranged kill zones, and then swarming against them. The Chechen units' ability to conceal themselves in Russian uniforms, hide among villagers, and infiltrate at night ensured that the Russians were constantly re-acting to Chechen attacks instead of achieving surprise. While securing key terrain, such as villages and roads, the Russians rarely "found" Chechen fighting elements, demonstrating the

[463] Arquilla and Karasik, "Chechnya: A Glimpse of Future Conflict?," 215.

[464] Ibid., 216.

challenges of the hider-finder paradigm in irregular conflict. While Russians would appear successful in the capturing of villages, Chechen fighters nearly always withdrew prior to the attacks and infiltrated back at night to launch devastating raids against the hasty Russian defenses.

b. Illumination

Russian intelligence should have been based on a need to illuminate Chechen forces using their social ties, operational activity, conducting infiltration, and through a focused exploitation campaign. However, Russian forces had extreme difficulty in generating even small bits of traditional intelligence on Chechen forces, let alone a comprehensive picture generated by extensive illumination efforts. Overall, the lack of Russian intelligence gathering efforts was one of the most glaring failures of the 1st Russo-Chechen war; much of was due to lack of coordination between the MoD and the *Federalnaya Sluzhba Kontrrazvedki*—Federal Counterintelligence Service of Russia (FSK), the Interior Ministry's counter-intelligence service. Since the MoD was not entitled to collection internal to the Russian Federation, by law, the Interior Ministry had the responsibility, but had little capability.[465] Most of the information that gathered by Russian forces resulted from traditional intelligence, and was delivered by anti-rebel Chechen opposition, which made it highly dubious. Although numerous Russian citizens lived in Grozny and the larger towns, Russian forces had little contact with anyone who could provide accurate local intelligence. In addition, the lack of understanding of the Chechen culture, and a dearth of Chechen speakers tremendously compromised their efforts. In strong contrast, Colonel Husein Iskhanov, General Maskhadov's deputy commander during the 1994–1996 war, stated, "we used our knowledge of the territory and our experience during military service with Russians. We knew how Russians built their defences; we knew Russian habits and language."[466] Further, most of the Russian efforts to identify Chechen fighters and supporters were based on harsh, repression measures. The Russians established "filtration" camps to separate Chechen fighters from

[465] Gall and de Waal, *Chechnya: Calamity in the Caucasus*, 208.

[466] Iskhanov, Interview from June 1999, 3.

ordinary citizens, but the overwhelming amount detained were civilians, who were subsequently beaten and tortured.[467] Testimonies from thousands held in such camps described, "…mass arrests from the streets and bomb shelters, irrational and cruel violence, including vicious beatings, mock executions, psychological and often physical torture to obtain confessions, and life-threatening conditions…."[468] Instead of establishing a system for obtaining information, the Russians had established the "…beginnings of a system of mass terror."[469]

c. Information Disruption

The Russians attempted to disrupt Chechen information strategy, but overall, as the Russian Federal Security Forces Chief, Sergei Stephasin bluntly stated, "the information war was lost."[470] Effective Russian information disruption would have displayed a significant ability to negate the Chechens' purpose, the denial or channeling of communications, collection, and deception efforts. In terms of countering the Chechens' purpose, the Russian invasion served to do almost the opposite, which swelled the initial band of Chechen fighters by thousands each week as fighters came to avenge the destruction caused by heavy Russian shelling. "Support for Dudayev came second to the desire to protect their homes and land. 'We are here because this is our fatherland,' said Apti Vasarkhanov, one fighter heading in [to Grozny] with a small group from his village. 'We have no choice, we have nowhere else to go.'"[471] As the war continued into the heaviest fighting of 1996, Russian media became increasingly muted, and Yeltsin's re-election campaign dominated most of the headlines. At the very same time that

[467] Gall and de Waal, *Chechnya: Calamity in the Caucasus*, 229.

[468] Ibid., 232.

[469] Ibid.

[470] Oleg Falichev, "FCS Will Certainly Publish Information on Who Helped Dudayev and How," *Krasnaia avezda*, January 21, 1995, 2, cited in Arquilla and Karasik, "Chechnya: A Glimpse of Future Conflict?," 217.

[471] Gall and de Waal, *Chechnya: Calamity in the Caucasus*, 222.

Russian forces were fighting one of the fiercest battles of the war, for the village of Goskoye, Yeltsin was informing U.S. President Bill Clinton, "military actions in the Chechnya region are not going on."[472]

d. Fusion

Russian forces displayed rigid, hierarchical organization, and little to no significant coordination between the various ministries, commanders, and separate units. The defining attributes of fusion, shared intent, connectivity, and collaborative systems were conspicuously absent at nearly all levels. One MVD unit was so angered by the lack of coordination and overall command influence that it packed up and departed Chechnya, believing there was, "no centralized control over the military operation."[473] Smaller units, *spetznaz* and other elite forces, may have displayed some elements of fusion, but for the most part, these were tactical derivations, with forces displaying local connectivity as a means of basic battlefield coordination. Fusion has both an organizational element and a doctrinal element, and because the Russians were unable to achieve even basic organizational connectivity, they were unable to establish any kind of collaborative systems.

D. THE 2ND RUSSO-CHECHEN WAR: 1999–PRESENT

After the brutal first conflict, and following an uneasy period of relative quiet, the 2nd Russo-Chechen War began with an Islamic extremist led offensive movement into neighboring Dagestan.[474] The Chechen leader Shamil Basayev and Saudi jihadist Ibn al-Khattab, who maneuvered over 2,000 fighters into neighboring Dagestan, led this large raid. This invasion, and five bombings throughout Russia between August 31 and September 16, 1999 killed over 300 people and wounded 2,1000, and produced a Russian

[472] Gall and de Waal, *Chechnya: Calamity in the Caucasus*, 316.

[473] Ibid., 209.

[474] Murphy, *The Wolves of Islam*, 2.

response—the return of the Russian Army to Chechnya.[475] Like the 1st Russo-Chechen War, this war was forecast to be a quick victory, and the Kremlin even described it as an "anti-terrorist" operation against Chechen rebels.

Beginning in Dagestan, the Russian forces slowly pushed the Chechen fighters under Basayev back into Chechnya, despite being continually ambushed. Prior to actually invading Chechnya, the Russian military paused to allow for artillery and aerial bombardment of targets, such as communication facilities and bases. In addition to striking these key military targets, infrastructure throughout Chechnya, such as dams, water treatment facilities, and bridges were destroyed and most larger towns were heavily shelled.[476] Russian forces entered northern Chechnya in a major offensive on September 30, 1999, and soon launched large-scale military operations against Grozny, and other major towns and their transportation routes.[477] A day later, Russian Prime Minister Putin officially declared war on Chechnya ordering Russian troops to use "all available means" to subdue the insurgents.[478] Russian operations were notable for their devastating approach, as forces used heavy bombardment to inflict enormous damage of Chechen cities, and Grozny in particular was nearly leveled. One retired Russian officer, Major General Vorob'yev stated that it took an average of 7,500 bullets and 70 rounds of artillery to kill one Chechen fighter.[479] By mid 2000, Russian forces had achieved a solid presence throughout Chechnya and had basic control of all major towns.[480] The taking of Grozny was a slow, deliberate affair, with an evacuation period and the methodical movement of heavy detachments from neighborhood to neighborhood, garrisoning

---

[475] Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 212.

[476] Charles W. Blandy, *Chechnya: Two Federal Interventions: An Interim Comparison and Assessment* (Sandhurst, UK: The Conflict Studies Research Center, 2000), 40, www.da.mod.uk/colleges/arag/document-listings/caucasus/P29.

[477] Tim L. Thomas, "A Tale of Two Theaters: Russian Actions in Chechnya in 1994 and 1999," *Analysis of Current Events* 12, no. 5–6 (2000): 2, http://fmso.leavenworth.army.mil/documents/chechtale.htm.

[478] Kramer, "The Perils of Counterinsurgency," 7.

[479] Charles W. Blandy, *Chechnya: Dynamics of War Brutality and Stress* (Sandhurst, UK: The Conflict Studies Research Center, 2001), 13, www.da.mod.uk/colleges/arag/document-listings/caucasus/P35.

[480] Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 212.

strongpoints as they proceeded. Still, it would be late March 2000 before Grozny was finally occupied, by which time, a large proportion of the Chechen insurgents had withdrawn to the mountains in the south. Building on the damage created in the 1994–96 war, the massive destruction throughout Chechnya resulted in the obliteration of its infrastructure, which left many towns and villages nearly uninhabitable.[481]

In turn, Chechen networks began a terrorist bombing campaign, with the notable incidents being the seizure of the Dubrovka theatre in Moscow in October 2002, in which 980 Russians were held hostage, and the taking of 1,300 hostages at the Beslan middle school in North Ossetia in September 2004. Both incidents culminated in large-scale raids by *spetznaz*, most likely the elite Russian unit *Alfa*, during which hundreds of civilians were killed. In September 2003, the overall command of Russian operations transitioned from the Federal Security Services (FSB), the Russian intelligence organization, to the MVD, a move meant to signify an end to counter-terrorism operations and more normal public security operations.[482] However, Chechen rebel networks worked hard to reverse the initial Russian gains, and inflicted enough damage against Russian forces that by 2005, they were successfully turning "tactical victories into strategic gains."[483] Chechen forces continued to display network-style warfare through swarming attacks in the North Caucasus, while at the same time, expanding their terrorist attacks in Moscow and other Russian cities outside of Chechnya.

In marked contrast to the first war, after several years of tough fighting, the Russian offensive focused on countering the Chechen guerrilla network by a combination of fixed conventional security positions, and aggressive pursuit by Russian *spetznaz*. In addition, the overall effort to target the Chechen network was led by intelligence organizations partnered with various special operations elements to initiate a "hunting" campaign.[484] This campaign was notable for the "…severe attrition inflicted over a

---

[481] Kramer, "The Perils of Counterinsurgency: Russia's War in Chechnya," 6.

[482] Graham H. Turbiville, Jr., "Hunting Leadership Targets in Counterinsurgency and Counterterrorist Operations," *Joint Special Operations University Report 07-6* (Hurlburt Field, FL: Joint Special Operations University Press, 2007), 64.

[483] Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 216.

[484] Murphy, *The Wolves of Islam*, 156.

decade on most of the best-known Chechen rebel field commanders, their subordinates, and jihadists and combatants who joined the fight against Russia."[485] Key leaders killed during this period included notable operatives, such as Ibn al-Khattab, a Jordanian born jihadist and operational commander killed in 2002, as well as Raduyev, who had been aggressively pursued since the Budinovsk raid. However, despite the fact that "….good intelligence and assistance was sometimes generated by FSB efforts to exploit differences among rival leaders and groups," and a significant number of key leaders killed or captured, much of the effort up until the September 2004 attacks in Beslan were sporadic.[486] The Beslan attacks prompted a tremendous re-organization of the Russian war-fighting structures for counterterrorism (inside Russian borders) and counterinsurgency (inside Chechnya). Chechnya was subdivided into 12 headquarter sections that employed a joint intelligence service in conjunction with special operations forces augmented by a motorized rifle company, a combat engineer team, and civil defense elements.[487] The successful combination of special operations forces and conventional elements is discussed in numerous sources on special operations, most notably James Kiras's *Special Operations and Strategy*, but such a robust joint force is rare.[488] In addition, a more clearly defined command structure facilitated the employment of regional special operations units with the national-level units, *Alfa* and *Vympel*.

The installation of Akhmat Kadyrov, a former Grand Mufti and insurgent, as the head of the provisional Chechen government in June 2000 helped with moderating the insurgency.[489] This began a fairly successful effort that built local networks of co-opted Chechens willing to relinquish their struggle in favor of local control. Akhmat Kadyrov's son, Ramzan, is the current prime minister of Chechnya, appointed in March 2006 after his father was assassinated by a bomb blast in a Grozny stadium. Still, efforts to

---

[485] Turbiville, Jr., "Hunting Leadership Targets in Counterinsurgency and Counterterrorist Operations," 52.

[486] Ibid., 59.

[487] Ibid., 65.

[488] James D. Kiras, *Special Operations and Strategy* (New York: Routledge, 2006), 3.

[489] Christopher Zurcher, *The Post-Soviet Wars: Rebellion, Ethnic Conflict, and Nationhood in the Caucasus* (New York: New York University Press, 2007), 98.

transition the bulk of the fighting to Russian-backed local police and pro-Russian Chechen security forces have been problematic due to their dubious loyalties and proven infiltrations at all levels.[490] Overall, these Russian efforts to develop larger Chechen-loyalist factions played a significant role in reducing the overall intensity of the conflict.

Like Dudayev, Maskhadov was a constant target of Russian assassination efforts, and special operations forces finally succeeded in targeting him in a joint operation composed of regional forces and the hastily deployed *Alfa* and *Vympel* teams. This operation consisted of regional forces cordoning the village of Tolstoy-Yurt, while the *spetznaz* teams, under the FSB commander General Aleksander Tikhonov launched "special weapons" rather than choosing to assault the structure.[491] Following Maskhadov's death in March 2005, and the rise of Abdul-Khalim Sadulayev to the ChRI leadership, the ChRI was further developed as a broad Caucasus jihad under the primary direction of one of the most notable combat leaders and terrorists, Shamil Basayev. "They [Sadulayev and Basayev] radically transformed the goals of the expanded war strategy and refashioned the national independence movement into an Islamist and increasingly globally-oriented jihadist movement…"[492] The targeting and killing of Sadulayev and Basayev in quick succession in June and July 2006 were serious blows to the Chechen fighters, and by the end of 2006, Russian forces had taken much of the impact out of the separatist struggle in the North Caucasus.[493] The success of the combined intelligence and special operations units led to an "unprecedented success in targeting and eliminating major guerrilla leaders," and President Putin to declare "officially" an end to the war in 2009.[494] Still, major terrorist activities continue and

---

[490] Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 264.

[491] Conflicting stories about the intelligence that led to this operation, as well as the conduct of the operation itself, are typical of many such high-profile Russian operations. It is likely that Maskhadov was located through electronic signals intercepts, which led to a "routine" passport check of the house. After receiving no response to a challenge, a bunker found under a hidden trapdoor inside was destroyed with the "special weapons," most likely thermobaric explosives. Turbiville, Jr., "Hunting Leadership Targets in Counterinsurgency and Counterterrorist Operations," 67–69.

[492] Hahn, "The Jihadi Insurgency and the Russian Counterinsurgency in the North Caucasus," 5.

[493] Turbiville, Jr., "Hunting Leadership Targets in Counterinsurgency and Counterterrorist Operations," 72–73.

[494] Ibid., 77.

activity under Doku Umarov, the 5th President of the ChRI and the "1st Emir of the Caucasus Emirate," included the March 2010 Moscow Metro bombings[495] and the January 2011 Domodedovo International Airport bombing,[496] both suicide attacks.

The Russian special operations successes in this campaign have shown a notable evolution beyond just heavy-handed destruction. However, such repression continued, largely by conventional forces and proved effective in exerting control over large areas of Chechnya. However, despite increased precision in targeting key leavers, the overall repressive nature of the Russian strategy leads most observers to believe that the war has simply entered a new phase. The current conflict is marked by dispersed, increasingly lethal terrorist attacks in the Russian heartland, and an expansion into neighboring provinces.[497] Daily attacks against Russian soldiers and facilities receive little or no mention in the press, due to strict state controls, but larger terrorist bombings and other strikes outside Chechnya continue to draw attention. Ironically, the vicious irregular warfare continuing inside Chechnya displays the remarkable ability of Chechen fighting networks, despite increasingly successful Russian counter-efforts.

1. Russian Invasion

Despite having several years to prepare for the replay, the Russian forces that invaded Chechnya in 1999 were once again unprepared for the strength and competence of their opponents. The Russians planned to avoid the bloody, vicious urban battles of their earlier incursion by forcing the Chechens into submission through artillery and air strikes. Once again, although mistaken assumptions justified a lack of preparation, and "…almost a complete lack of to urban combat in preparatory training" for most Russian conventional units.[498] Russian main-line units were augmented by *kontrakti*, contracted mercenaries, as well as buttressed by multiple elite units that aided in combating the agile

---

[495] "Chechen Rebel Says He Ordered Moscow Metro Attacks," *BBC News*, March 31, 2010, http://news.bbc.co.uk/2/hi/8597792.stm.

[496] Steve Rosenburg, "Chechen Warlord Doku Umarov Admits Moscow Airport Bomb," *BBC News*, February 8, 2011, http://www.bbc.co.uk/news/world-europe-12388681.

[497] Fogarty, "Chechnya Redux? Violent Conflict in Ingushetia."

[498] Oliker, *Russia's Chechen Wars 1994–2000*, ix.

Chechen forces, but whose effect may be marginalized by the overall repressive nature of Russian COIN. As the war progressed, re-organization and an increasing reliance on combined special operations and intelligence units led to increasing successes against Chechen leadership figures.

Organizationally, the Russian forces were organized under a single MoD command, which simplified and improved command and control. This organization was still largely a hierarchical structure based on traditional organizations, but it displayed greater unity through the "Unified Grouping of Federal Forces," (OGV) which had responsibility for all military and security forces in Chechnya, and was divided into four different sectors. By January 2001, a transfer of authority occurred from the MoD to the FSB, when President Putin declared the military phase of the campaign over, to mark the shift from full-scale combat operations to a basic counter-terrorism mission.[499] The FSB ran all counter-terrorist efforts in Chechnya for two-and-a-half years, before President Putin transferred full responsibility to the MVD in July 2003. While still under a "unified" command, the OGV was headed by a MVD general, who attempted to manage multiple staff and operational elements from the MoD, as well as FSB operations.[500] This structure involved multiple ministries, agencies, and branches, which provided for an increase in overall coordination of diverse joint operations. However, despite a more integrated command structure, designed to facilitate more effective and synchronized operations, major coordination issues remained. After a large raid against Russian positions in Ingushetia in June 2004, the Russian State Duma Committee on Security held that the "…lack of coordination among the federal and regional security services and the army," was the reason that "allowed the terrorists to strike at Russian units with impunity."[501] This lack of coordination led to the creation of a new federal-level commission to coordinate the primary ministries of the military, FSB, foreign intelligence

[499] Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 217.

[500] Ibid., 218.

[501] Comments of committee chairman Viktor Illyukhin and committee member Grennadii Gudkov, cited in Igor' Plugatarev, "Ukhod nachal'nika Genshtaba Kvashnina predopredelen: Kreml' gotovitsya nazvat' osnovnogo vinovnika za sluchivsheesya v Ingushetii," *Nezavisimoe voennoe obozrenie*, no. 24, July 2, 2004, 1–2; cited in Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 219.

service (SRV), and military intelligence services (GRU). The commission was reinforced by President Putin's formation of the National Anti-Terrorist Committee (NAK) in February 2006, which gave broad powers to coordinate and develop "new methods and approaches for countering terrorism."[502] In addition, the NAK formed an operational staff—the Federal Operational Staff (FOSh) to bring together forces and resources, as well as share intelligence. This staff supported 12 new federal headquarters, designated as an Operational Control Group (GrOU) that had responsibility for each North Caucasus administrative region. These GrOUs function as a joint task force, and are designed to have assigned forces from various units and agencies, which support the following typical organization composed of the following.

a. Motorized Rifle Company

b. 70-man MVD police *spetsnaz* detachment (quick reaction)

c. Combat engineer team

d. Civil defense/emergency troops and resources for rescue and construction work

e. So-called 'heavies' or special operations teams comprised of elements from the North Caucasus FSB directorates, designated as *spetsnaz*[503]

The same pressure for organizational redesign also led to the development of special designation forces under the GRU, two battalions whose ethnic Chechen composition made them well-suited to their task of "liquidation of suspected insurgents." These battalions are referred to by their sector designations, East (*Vostok*) and West (*Zapad*) and have been accused of numerous war crimes and atrocities.[504]

Doctrinally, the Russian forces adapted from the 1st Russo-Chechen war by determining that they would not engage in the close-quarters urban fighting that proved so devastating in Grozny and other urban areas. Instead, they based much of their doctrine on using stand-off firepower, artillery, aerial bombardment, and even new

[502] Hahn, "The Jihadi Insurgency and the Russian Counterinsurgency in the North Caucasus," 10.

[503] Turbiville, Jr., "Hunting Leadership Targets in Counterinsurgency and Counterterrorist Operations," 65.

[504] Ibid., 63.

munitions, such as fuel-air explosives, to raze urban areas and eliminate any threat they might contain. However, the expected artillery and air strikes failed to lead to a decisive victory in Grozny and other urban areas, and there were no other plans. "The key mistake the Russian military made between the wars was in drawing the wrong lesson from urban combat: not only that it should be avoided, but that it could be avoided, under all circumstances. They were therefore unprepared for it when it came."[505] In addition, they increased their focus on leadership targeting, as evidenced by the formation of joint groupings and expanded use of elite units. These units and their targeting efforts provide much of the successes heralded by the Russian media, and the combination of the two has proven fairly effective in swaying opinions about the conflict. Further, the increase in techniques, such as "countercapture" operations, which were directed against the families of accused terrorists. Such operations, while seemingly increasing pressure against the Chechen fighters, also led to widespread condemnation by Russian human rights groups and international organizations, while at the same time, adding to the hostility and hatred among Chechen civilians.[506]

Operationally the Russians made changes to the way in which they fought the Chechen networks. The noteworthy changes included a dramatically increased use of heavy shelling and bombardment of urban areas, decentralized authority and mixing of units, hardening defensive positions, and an increase in the operational employment of elite special operations forces. Heavy use of massed firepower and standoff limited Russian casualties, but produced a tremendous amount of devastation in infrastructure and noncombatants. Russian forces employed devastating amounts of direct and indirect firepower to destroy built-up areas as they believed that force preservation was far more important, based on the loss of public support due to horrendous loses in the first war. Russian forces also sought to create more effective units when they did have to fight. Russian assault groups decentralized authority to junior officers, which resulted in small units with increased effectiveness and survivability. In addition, "increased use of

---

[505] Oliker, *Russia's Chechen Wars 1994–2000*, xiii.

[506] Turbiville, Jr., "Hunting Leadership Targets in Counterinsurgency and Counterterrorist Operations," 63.

specialized units [special operations forces] to backstop the mostly conscript motorized rifle troops improved effectiveness and decreased casualties and fratricide."[507] Russian forces also concentrated on countering the attrition and psychological toll inflicted by the Chechen swarming ambushes. Much of this effort focused on installing dense minefield and explosive barriers, as well as early-warning devices along all roads leading to military posts and bases. However, this increasing reliance on fixed bases and superior firepower may not provide much advantage against the agile Chechen forces:

> The large and powerful but disorganized federal units, which are devoid of any genuine support among the local [Chechen] population, often have been powerless when confronted by much smaller but mobile bands of guerrillas in the region….[The Russian government] usually gauges its military strength [in Chechnya] by tallying up the numbers of soldiers, tanks, guns and helicopters, but experience shows that in Chechnya—and in the North Caucasus more generally—all of these indicators are of little relevance. Our troops, aside from trying to protect themselves against attack, are often unable to do anything.[508]

Much of the heavier fighting, especially in the mountainous southern areas of Chechnya, has been borne by elite elements, as a senior GRU officer stated, "the GRU *spetznaz* forces have had to undertake at least half of all federal operations [in Chechnya] because no forces other than the *spetznaz* dared venture into the mountainous regions."[509]

The Russians demonstrated remarkable improvements in their information strategy for the second war, perhaps the most notable adaptation from the first war. Most of these changes were focused on how they dealt with the media, both internally and globally. While the 1st Russo-Chechen war displayed the information openness of glasnost, in the second conflict, Russian authorities exerted strict control of the press and a remarkably professional public relations campaign. Moreover, in the 2nd Russo-

---

[507] Oliker, *Russia's Chechen Wars 1994–2000*, xiii.

[508] Vadim Rechkalov, "'Budut lokal'nye stychki s Zhertvami do 100 chelovek, a voiny ne budet': Bandformirovaniya Severnogo Kavkaza osvaivayut novuyu takitu," *Izvestiya*, August 2, 2004, 1, cited in Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 224.

[509] Vladimir Mukhin, "V Chechne voyuyut glavnym obrazom spetspodrazdeleniya," *Armeiskii sbornik*, July 7, 2003, 32–33, cited in Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 212.

Chechen war, the Russians placed a great deal of emphasis on Chechen "excesses" and highlighted the vicious nature of the Chechen terrorist actions, as well as their use of "barbaric" battlefield executions.

2. Chechen Response

Overall, the Chechen fighting networks have continued to display many of the same characteristics that emerged in the first conflict. They continue to be a part of the strong social networks, which compose Chechen clan-based society, and draw support from this base. Their swarming tactics continue to impose significant loses against Russian forces, particularly in the complex and potent ambushes of Russian forces attempting to move throughout Chechnya. They have also continued the expanded form of the conflict, with dramatic raids throughout the Caucasus region, and terrorist attacks that strike throughout Russia. If anything, the increased Russian pressure and forcible occupation of the region has led to an increasingly dispersed Chechen fighting structure, one that actually enjoys considerable freedom of movement throughout the countryside, especially in the southern mountains. They continue to rely on their ability to travel using Russian documents and many of the terror attacks in Moscow and other cities are simply an extension of Chechen units, which rely on small clandestine supporters and individuals who either travel for the attack or reside in larger Chechen communities. Despite their sophisticated methods and technical armament, Chechen insurgent networks are notable because they have not received formal recognition, or external support. They obtain most of their weapons and supplies from Russians, either in raids on arms depots, or in buying them from Russian troops, and have accumulated significant stockpiles in the Northern Caucasus. As Mark Kramer states, "the conflict in Chechnya belies the notion that major insurgencies can endure for many years only if they receive large-scale external backing. That may have been true of the guerrilla movements in South Vietnam in the 1960s, Afghanistan in the 1980s, and Kashmir in the 1990s, but it is not true of Chechnya since 1994."[510]

[510] Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 260.

Organizationally, the 2nd Russo-Chechen war displayed an increase in autonomy by Chechen units and a less formal, centralized authority than that displayed by Dudayev's initial version of the ChRI in the first war. In July 2002, President Maskhadov held a war council where the increasing jihadization of the Chechen separatist movement was formalized through amendments to the constitution establishing *shariah* as the official law for the underground republic.[511] This action formalized the increasing emphasis on a jihadist ideology, which had been growing due to the risk in ranks of young, radical Islamists who were influenced by the global Islamist movement. With this shift, the leadership began to create more combined units, composed of foreign mercenaries, al-Qaeda operatives, and indigenous Chechen militant units.[512] This change was a departure from previous divisions between more strictly nationalist-oriented Chechen separatists and the jihadist-bent fighters. The current war has brought leaders to the forefront who espouse an unreserved jihadist agenda, and increased the influx of foreign militants who claim to be fighting on behalf of a wider, global Islamic community.[513] Overall, the Chechen separatists remain a decentralized, networked organization, with elements becoming more autonomous and smaller over the last five years. The combined units have served to increase their ranks, while still allowing them to maintain connections with the strong clan-based social networks. The combination of this strong social infrastructure and well-trained, global jihadists provides a complex organizational grouping.

Doctrinally, the Chechens continue to rely on their ability to swarm, and have merged this with an increasing focus on dramatic terror strikes to achieve devastating results in raids like the one in Beslan in 2004. This swarming capability is especially notable as pro-Russian forces have increasingly adapted a strong-point approach, with forays occuring from heavily fortified positions. The Chechen willingness to fight at

---

[511] Sharia is Islamic law, as described in the Quran, but is interpreted in multiple ways and usually violently enforced by militant jihadists, as described in Fawaz A. Gerges, *Journey of the Jihadist: Inside Muslim Militancy* (Orlando, FL: Harcourt, 2006), 10–18. Hahn, "The Jihadi Insurgency and the Russian Counterinsurgency in the North Caucasus," 3.

[512] Hahn, "The Jihadi Insurgency and the Russian Counterinsurgency in the North Caucasus," 3.

[513] Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 259.

night continues to give them an upper hand against nearly all Russian units. Most Russian forces remain in static positions at night, which allow Chechen raids and extensive prepositioning for ambushes. The notable extension of the war outside the Chechen region is seen in terrorist attacks involving suicide bombings, remotely detonated bombs, and hostage-taking operations. Chechen doctrine seems to be focused on maintaining the offensive inside Chechnya, while extending it with dispersed and violent attacks throughout the Caucasus region and the rest of Russia.[514] In a variation of swarming, Maskhadov promoted the "tactic of the bee," which involves rotating the focus of the jihadi attacks from one republic to another, which is designed to keep Russian security efforts disrupted.[515] This effort has seen the attacks shift from Chechnya, to Ingushetia, to Dagestan, Russia itself, and then back in a seemingly random manner. A 2004 nighttime raid by Basayev and Dokku Umarov into Ingushetia that resulted in severe casualties and the capturing of large quantities of weapons, ammunition, and supplies is a notable example.[516] These actions are consistent with their overall strategy of prolonging the "stalemate" while raising the overall costs of the war, to the point that the Russians will reshape their calculations, as they did in 1996.

Operationally, the Chechen forces continue to utilize many of the same methods that they displayed in the first war, with an increase in two types of attacks—roadside IEDs and suicide bombings. The first, a dramatically increased use of mines and IEDs, reflects both their ability to emplace such explosive devices stealthfully, as well as the Russian reliance on more static positions supported by road arteries. The 'mine warfare' employed by the Chechen fighters presented serious problems for Russian troops, causing an estimated 40% of the casualties they have suffered during the latest war.[517] Colonel-General Nikolai Serdtsev, the head of the Russian Army's Engineering Forces, states that the challenges faced by demining grew much greater than that seem in from 1994–1996:

---

[514] Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus" 216.

[515] Hahn, "The Jihadi Insurgency and the Russian Counterinsurgency in the North Caucasus," 3.

[516] Turbiville, Jr., "Hunting Leadership Targets in Counterinsurgency and Counterterrorist Operations," 60.

[517] Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 226.

> If we compare the scale of the 'mine war' in the current campaign with the earlier one, we find that the intensity of it has sharply escalated and the number of casualties among our combat and technical personnel has sharply increased. All of this confirms that the terrorists are now more organized in their preparations, in their accumulation of stockpiles of high-explosive munitions, in their development of a network of clandestine laboratories to construct improvised explosive devices and radio-controlled detonators, and in their plans for laying mines and explosive devices.[518]

It is likely that this increase in IEDs is a result of doctrinal innovations from Iraq, diffused mainly through cyberspace, but also an exchange of fighters.[519]

Suicide attacks also dramatically increased, as Chechen forces became more infused with jihadist ideals extolling such attacks. These attacks began in 2000, and were initially directed at individual Russian troops, or groups manning checkpoints. They quickly shifted to larger attacks against headquarters with the use of vehicle-born explosives (referred to in U.S. nomenclature as suicide-vehicle-born improvised explosive devices—SVBIED), and have resulted in hundreds of large-scale bombings throughout Chechnya. By 2004, these tactics had spread throughout the entire Caucasus region, with suicide bombing and other large-scale explosive attacks forming a key aspect of Chechen operations in a "widened zone of combat operations," in Ingushetia, Dagestan, North Ossetia, and other regions.[520] Terrorist attacks against targets deeper inside Russia have had a dramatic effect, and their escalation in 2003–2004 marked a different type of war. "In 2003 alone, nine suicide bombings in Moscow were attributed to the Chechens, and more than 600 other terrorist bombings occurred elsewhere in

---

[518] Interview with Serdtsev in Sergei Konovalov, "Kontrterroristicheskaya operatsiya: Voennye i militsiya podelili Chechnyu na zony otvetstvennosti," *Kommersant*, January 19, 2004, 6, cited in Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 226.

[519] Cooperation between Iraqi jihadists, notably al-Qaeda in Iraq and Chechen jihadists, is evident in the request for action by Chechens against Russians in Iraq and the subsequent execution of five "Russian diplomats" and "spies" in Baghdad in June 2006. Shamil Basayev noted that these deaths were exacted in revenge for the Russian assassination of former Chechen President Zelimkhan Yandarbiyev in Doha, Qatar in 2004. The execution of the Russian diplomats likely played a role in the increased focus and resources devoted to targeting Basayev and others, leading to his death a month later. Turbiville, Jr., "Hunting Leadership Targets in Counterinsurgency and Counterterrorist Operations," 2–3.

[520] Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 245.

Russia, especially in or near the North Caucasus."[521] Chechen fighters also continued to dominate using night ambushes against Russian forces. Their night-fighting prowess was a strong contrast to Russian forces both under-equipped and un-trained for such fighting, which made small-unit warfare even more salient in the latest conflict.

Chechen information strategy seeks to capitalize on Chechen operational effects by highlighting the Chechen cause. By increasing terrorist attacks, the Chechens have managed to keep the conflict in the spotlight, but such attacks have had mixed results, as they have hardened Russian opinions and allowed President Putin to draw strict comparison with other terrorists, such as al-Qaeda. In addition, the Russian blackout on the state media coverage of the war has hurt the Chechen efforts to keep their message and efforts visible. Strict control of journalistic coverage and the overall increase in lawless violence in Chechnya also contribute to less ability to reach outside opinions.

2nd Russo-Chechen War				
	Organization	**Doctrine**	**Operations**	**Information Strategy**
Russian Forces	*Hierarchy *Improved Coordination *Chechen Partnerships	*Methodical, Linear Advance *Overwhelming Force *Avoid Urban Combat	*Stand-off Firepower *Fortified Outposts *Special Operations	*Media Denial *Official Narrative
Chechen Forces	*Decentralized *Dispersed Cells *Increased Autonomy	*Swarming *Terror Campaign	*Synchronized Attacks *Capable Small Unit Tactics *Suicide Attacks *IEDs	*Weakened Narrative *Reduced Media Access *Jihadist Ideology

Table 6. Evaluation of the 2nd Russo-Chechen War

[521] Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 247.

3. Analysis of Counter-Network Model

a. Offensive Swarming

Russian efforts to counter Chechen fighting networks in the 2nd Russo-Chechen war demonstrated significant improvements from the mostly traditional stumbling of the 1st Russo-Chechen War. Overall, although the larger Russian doctrine continued to focus on the use of heavy weapons and destruction of Chechen urban areas as a means to deny terrain and avoid fighting against the Chechen bands. This doctrine has largely mitigated the wasteful casualties that resulted in initial attempts to take Grozny, but it has not necessarily resulted in any significant loss to Chechen fighters. Chechen losses are largely the result of improved targeting outside the traditional siege mentalities clearly displayed in the first years of the war. A significant portion of this improvement was the use of special operations forces in a manner that resembles offensive swarming, mostly due to their ability to achieve surprise. However, the employment of these elite forces was more attributable to deliberate shooting than a faster rate of fire, and never generated significant operational tempo. Largely because of organizational inefficiencies and a lack of supporting illumination and fusion efforts at the operational level, overall targeting of the Chechen networks continues to be at a pace at which Chechens can rebound.

b. Illumination

Russian intelligence continues to be marked by significant issues and problems in coordination between the FSB and MVD. Both organizations continue to be at odds with each other, and reluctant to share information, contributing to the Chechens frequent success with terrorist attacks. Overall activities that resemble illumination are attempts at increasing Chechens' operational activity in rural areas, and a very heavy-handed use of exploitation. The deployment and increased usage of unmanned aerial vehicles (UAVs) brought ISR capability to the battlefield, and increased the Russian's ability to identify operational activity. Still, without an overall collaborative system to tie into, these UAVs were primarily employed in a defensive role around static bases.

Russian exploitation efforts focused on repression mass arrests aimed at weeding out fighters from a larger civilian population, but these crude efforts to identify fighters provided little in the way of actual exploitation on the Chechen fighting network. On the whole, attempts at infiltration and the use of social ties have been significantly absent as well since efforts to recruit Chechens have failed disastrously in the past, and they are barely trusted enough to be recruited, let alone infiltrate back into opposition networks.[522] A notable exception is the use of agents in the special operations targeting campaigns, such as the infiltrator who delivered the poisoned letter that killed Ibn al-Khattab.

c. Info Disruption

The primary aspect of information disruption seeks to negate a networked opponent's sense of purpose, which is critical to weakening the overarching ideas and goals, or narrative that is so instrumental in maintaining a cohesive network. The Russian efforts in the 2nd Russo-Chechen war seemed to actually strengthen the Chechen resistance, and their repressive methods actually expanded the overall size of the fighting network and attracted numerous foreign fighters. In some ways, the Russian government sought to negate the Chechen message by referring to the conflict as a "counter-terrorist operation," and refusing to acknowledge separatist claims.

The Russian effort at media denial has clearly been one of the most important factors in accounting for an overall lack of public protest against the 2nd Russo-Chechen war. During the 1994–1996 war, independent TV stations broadcast at will, but during the latest conflict, the Russian government imposed stringent controls over all media broadcasting. In addition, the "right" Russian message is getting out, with Russian news programs focusing on Chechen acts of terror and the heroic exploits of Russian troops. However, the Russians focused less on the Internet, whereas Chechen-controlled sites remained active, and overall, paid little attention to the Internet as a

[522] Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 249–250.

communications medium.[523] In addition, as time goes on, the initial heroic accounts have lost some of their luster, especially as reports of success became less credible and official accounts did not list mounting losses.[524] Tactically, the Russians displayed some advances in the second war by fielding more electronic warfare units, and improvements in training and equipment made it far easier to track the source of transmissions, as well as jam them.

Collection by the two primary intelligence agencies has been remarkably ineffective, and is primarily limited by the lack of Chechen language capability. Very few intercepted communications are ever translated, and during the October 2002 hostage crisis, the FSB was able to intercept all the terrorist phone conversations, but was unable to understand them. A prominent Russian journalist, Vadim Rechkalov, noted that, "during the many times I have been to Chechnya over the past several years I have never met even a single Russian soldier or FSB official who knew the Chechen language."[525] Deception as a tool of information disruption seems to follow the lack of ability to acquire and understand Chechen communications. However, one deception success story at the tactical level involved a Russian transmission about a false attack from the east, and when the rebels reinforced in the direction of the expected attack, they were ambushed, killing 20 and wounding another fifty.[526]

d. Fusion

The creation of the OGV represents an attempt to provide more unity of command and an increased connectivity among different forces. These efforts were also seen in Russian exercises designed to increased joint cooperation, such as the exercise in July 1998 that spanned the territories of Dagestan, North Ossetia, Ingushetia, Karbardin

---

[523] Pavel Chernomorskiy, "Second Chechen War on the Internet: Total defeat?" (in Russian), *Internet.ru*, February 18, 2000, http://www.internet.ru/preview_a/articles/2000/02/18/1760.htm; cited by Oliker, *Russia's Chechen Wars 1994–2000*, 63.

[524] Oliker, *Russia's Chechen Wars 1994–2000*, 64.

[525] Vadim Rechkalov, "'Budut lokal'nye stychki s zhertvami do 100 chelovek, a voiny ne budet': Bandformirovaniya Severnogo Kavkaza osvaivayut novuyu taktiku," Izvestiya, August 2, 2004, 1, cited by Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 250.

[526] Oliker, *Russia's Chechen Wars 1994–2000*, 52.

Balkaria, and Stavropol, in which MVD commanders exercised some 15,000 troops from the MoD, MVD, Border Guards, FSB, and other forces.[527] However, rivalries between the main intelligence organizations, corruption and lower-mid levels, and differing views on the goals and methods for prosecuting the war in Chechnya make attempts at fusion difficult. The key elements of fusion are shared intent, connectivity, and collaborative systems, and Russian forces demonstrated significant weaknesses in achieving any of these aspects. The lack of shared intent among Russian forces manifests itself in the rivalries and divisions between the primary intelligence agencies. As Olga Oliker states, "…serious problems remained between MVD and MoD units and between Russian troops and Chechen loyalist militias. These problems were compounded by distrust among the various groups. Moreover, even with a single commander at the top, there were too many generals contributing to the confusion."[528] Further, "many, if not the majority of the Russian soldiers serving in Chechnya no longer have a clear idea of what they are fighting for, and this problem will only grow more acute as the war drags on."[529] The Russians have made attempts at connectivity, most notably the FOSh intelligence-clearing center, where they have brought together terrorism analysts from each of the Russian special services and agencies for monitoring and forecasting of terror-related activities.[530] These efforts, combined with Russian elite forces targeting, have provided a sense of overall effectiveness, and at the least, demonstrate significant improvement since the dramatic terrorist attacks in 2004 and 2005.

4. Results of 2nd Russo-Chechen War

The Russian army displayed significant improvement between the 1st and 2nd Chechen wars, but overall, these improvements were not primarily aimed at effective counter-network operations. The bulk of the Russian forces focused on very traditional

---

[527] Valentina Lezvina, "Exercises in the Caucasus," (in Russian), *Kommersant-Daily*, July 21, 1998, FBIS-UMA-98-217, cited in Oliker, *Russia's Chechen Wars 1994–2000*, 37.

[528] Oliker, *Russia's Chechen Wars 1994–2000*, 51.

[529] Thomas E. Graham, Jr., "Can Russia Win in Chechnya," *Brown Journal of World Affairs* 8, no. 1 (Winter/Spring 2001): 6.

[530] Hahn, "The Jihadi Insurgency and the Russian Counterinsurgency in the North Caucasus," 10.

operations designed to seize and hold terrain. Urban terrain was simply destroyed to reduce its complexity, and once terrain was secure, it was physically strong pointed. The occupation of Grozny in the second war, while still horrendous, was much less costly for Russian troops than their earlier penetrations. By avoiding urban conflict, the Russians eliminated terrain that enabled the Chechens to maximize their swarming doctrine. A notable contrast between the two wars was the Russian blockage and manipulation of the media, and overall, it may have provided the greatest strength to Russian efforts.

As the war progressed, and especially after the large terror attacks, most notably Beslan in 2004, Russian command and ministries were forced to re-evaluate their ability to coordinate and share intelligence. Once much of the key terrain within Chechnya was seized, Russian efforts shifted to a "counter-terrorism" focus, in which their performance shows some good efforts to perform effective counter-network operations. This focus on intelligence collection, with its main effort focused on stopping attacks inside Russia, provided additional connectivity and slightly better coordination. The increased use of specialized troops and a greater intelligence focus provides an example of doctrinal improvement, but while their role highlights the requirement for such efforts, it is still fairly rudimentary. Russian efforts to quarantine the Chechen conflict with a media blockade continue, and allow the Russians to determine much of the global public opinion about the Chechen conflict. The installation of Kadyrov as the head of the provisional Chechen government has allowed for success in "Chechenizing" the conflict. This success is definitely mixed, however, as much of the loyalist Chechen forces are heavily infiltrated and the lack of a reliable police force contributes to a security vacuum within the region, with crime and overall disorder more prevalent than any effective security.[531] Still, despite continued fighting throughout the Caucasus region, and dramatic terror attacks in the Russian heartland, many Russians accept Putin's declaration that the war ended in 2009, which reflects higher levels of Russian control.

Overall, the 2nd Russo-Chechen war showed the importance of information on the conflict, through tight media restrictions, a slight trend towards better coordination and intelligence sharing, and a consistent requirement for elite units able to match the

[531] Kramer, "The Perils of Counterinsurgency," 11.

flexibility of Chechen fighters. In addition, it demonstrates the remarkable resiliency of the Chechen fighting networks. This resilience is even more noteworthy given the Russian strategic advantages and proximity, and demonstrates that major insurgencies do not necessarily require large-scale external backing.[532] Despite Russian occupation of the country and the installation of a pro-Russian Chechen government, the Chechen fighting networks have continued to conduct dramatic attacks.[533]

E. CONCLUSION

The Russian experience in the 1st Russo-Chechen War highlights the sheer unsuitability of attempting to fight a highly networked opponent in a traditional manner. The Russians were soundly defeated in their attempt to subdue Chechen fighting networks. During the course of the war, the Russians adapted better small-unit tactics and sought to bypass or destroy villages rather than engage in urban fighting. However, overall, little display of effective counter-network operations occurred. The Russian forces fought largely in a traditional manner, with little to no application of common COIN principles. No attempt was made at "winning hearts and minds," although it is doubtful that such efforts would have resonated with the Chechens.

Russian performance in the 2nd Russo-Chechen War provides varying degrees of contrast. Improvements in the capabilities of operational groups, the co-option of Chechen loyalists and use of *kontrakti*, and greater employment of elite forces, all provided additional capability. However, despite these improvements, Russian forces continued to rely on heavy firepower as a primary measure, which was employed to protect Russian soldiers, as well as reduce the Chechen's resolve to fight in urban areas. The increased terror threat forced a focus on counter-terrorist operations. It also displays the capabilities of Russian special operations, greater synchronized command and control, and some integration of intelligence. The Russians have been able to obtain a

[532] Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus," 260.

[533] Ibid., 267.

measure of security in Chechnya, largely as the result of transferring responsibility to a Chechen provisional government, and continued repression, but they still face a capable, dispersed, and radicalized Chechen fighting network.

Russian Counter-Network Performance				
	Offensive Swarming	Illumination	Information Disruption	Fusion
1st Russo-Chechen War	-	-	-	-
2nd Russo-Chechen War	-	+	++	+

Table 7. Overall Russian Performance against Chechen Fighting Networks[534]

The Russians never sought to swarm against the Chechen networks; instead they preferred a combination of traditional warfare and counter-terrorist operations best described as leadership targeting. The reasons for this lack of offensive swarming are most likely the overall weakness of Russian forces in small-unit tactics and larger organizational requirements that dictate firm control of maneuver units. The counter-leadership efforts of the 2nd Russo-Chechen war provide notable successes on a regular basis, but do not appear to be occurring at the pace required to generate a disruptive operational tempo.

Significant gaps in Russian understanding of Chechen culture and a lack of language capability provide the fundamental weakness in any Russian attempts at illumination. While the Russians have utilized some of the aspects of illumination, such as operational activity, their blunt, repressive attempts at acquiring information through exploitation create more resentment than anything else. In addition, it would appear that the cooperation with large numbers of Chechen proxy forces would increase illumination efforts, but it appears that this is a double-edged sword, with large levels of corruption and infiltration preventing the necessary trust.

[534] This basic table highlights the Russian performance of a few aspects of the counter-network variables, and the differences in their approach to each conflict. The addition symbol (+) indicates performance with a highly effective performance assigned three symbols (+++).

Russian attempts at achieving fusion are seen in efforts to increase overall coordination between the major ministries, as well as in efforts at the tactical and operational levels in their counter-leadership targeting efforts. These basic organization steps are improvements to the lack of unity and little coordination in the first war. However, the connectivity required for the organizational component of fusion may not be achievable given the intense rivalries and distrust between various organizational structures. Doctrinally, little evidence indicates that the Russians understand the requirement for collaborative systems merging operations and intelligence, except at the most tactical level.

Russian efforts at shutting down media access to the Chechen conflict and disseminating only officially approved news show a dramatic improvement from the almost complete lack of information awareness displayed in the 1st Russo-Chechen war. This change is the most significant between the two wars, and demonstrates an understanding of basic information age principles. A lack of language and cultural understanding contributes to their inherent weaknesses in collection and denial capabilities.

Overall, Russian forces showed some improvements in coordination and doctrine between the 1st and 2nd Russo-Chechen wars. Analyzing this case study using the proposed counter-network framework shows that the Russian performance improved somewhat in the 2nd Russo-Chechen war and slight degrees of performance occurred with respect to the primary independent variables. Mostly,, the Russians displayed increased coordination and an increased a greater agility through the use of special operations units. Increased efforts at network-style warfare are further seen in the relationships formed with Chechen loyalists and the dramatic changes in Russian information strategy. Still, even in the 2nd Russo-Chechen war, Russian forces fought in a mainly traditional manner, or with a strict leadership targeting focus. They achieved a greater degree of control through a COIN strategy that used brutal repression to secure

areas, while building partnerships with pro-Russian Chechens.[535] The Russian effort in Chechnya, to date, has largely suppressed the secular secessionist movement, co-opting most of it into a loose confederation run by the repressive Kadyrov. However, even this pro-Russian element of society has turned into an anarchic region, based on competition between warlords, gangs, and Russian security services, displaying "…underlying trends which are gathering momentum as a result of an increasing cycle of violence."[536] Further, the increasing terror attacks throughout Russia are a clear sign that the Chechen fighting networks have grown more extreme, despite being increasingly isolated.

[535] Thomas Ricks, "Counterinsurgency: The Brutal but Effective Russian Approach," *Foreign Policy*, September 17, 2009, http://ricks.foreignpolicy.com/posts/2009/09/17/counterinsurgency_the_brutal_but_effective_russian_approach.

[536] Charles W. Blandy, *North Caucasus: Negative Trends* (Shrivenham, UK: Defence Academy of the UK, 2009), 2. www.da.mod.uk/colleges/arag/document-listings/caucasus/09%2812%29%20CWB%203.pdf.

V. ISRAELI-HEZBOLLAH CASE STUDY

> So the best fortress that exists is to avoid being hated by the people. If you have fortresses and yet the people hate you they will not save you; once the people have taken up arms against you they will never lack outside help.[537]
>
> - Niccoló Machiavelli

> Some speak about the resistance's weapons as being separate from the resistance itself; [but] weapons without the resistance have no value. The real value of the resistance and its religious and national duty is its humanity…the weapons come after all this.[538]
>
> - Sayyed Hassan Nasrallah

A. CASE STUDY OVERVIEW

This case study focuses on the Israeli conflict with Lebanese Hezbollah, and in particular, analyzes the results of the Israeli occupation of Lebanon from 1982–2000 and the 2006 Israeli-Hezbollah. This examination of Lebanese Hezbollah is multi-faceted and considers both regional and global actions, acknowledging that Hezbollah's activities are globally dispersed. It is recognized as a terrorist organization, as Central Intelligence Agency (CIA) Director George Tenet stated, "Hezbollah, as an organization with capability and worldwide presence, is equal [to al-Qaeda], if not a far more capable organization. I actually think they're a notch above in many respects."[539] However, Hezbollah is much more than just a terrorist group, and its complex diversity defies many traditional descriptions. From its inception in the early 1980s, Hezbollah has been a violent non-state actor, acting with support from various sources, but always characterized by a popular socially based militant movement focused on resisting the

---

[537] Niccoló Machiavelli, *The Prince*, trans. George Bull (London: Penguin Books, 1999), 93.

[538] Sayyed Hassan Nasrallah, "We Will Consider Any Hand that Tries to Seize Our Weapons As An Israeli Hand," in *Voice of Hezbollah: The Statements of Sayyed Hassan Nasrallah*, ed. Nicholas Noe (Princeton, NJ: Princeton University Press, 2007), 338.

[539] U.S. Senate Committee on Armed Services, *Current and Future Worldwide Threats to the National Security of the United States*, February 12, 2003.

actions of Israel and its supporters.[540] In this sense, it is an instructive case, because it highlights the character of irregular warfare, with a non-state actor challenging national powers by directly confronting their military forces.

This case is examined in two main sections, which focuses primarily on Israeli-Hezbollah interaction, but also includes Hezbollah global support activities and terror attacks. The first section of the case concentrates on the initial stage of the conflict, beginning with the formation of Hezbollah in 1982 and its role in driving Israel from southern Lebanon. The last units withdrew in 2000. This first section briefly examines the initial invasion and fighting against the Palestinian Liberation Organization (PLO) to provide a basis for comparison with efforts against Hezbollah, as well as to show that these events were not independent. The invasion created the Hezbollah Shi'a threat, and the 1982–2000 conflict, which was emerging nearly simultaneously with the Israeli fight against the PLO. The second section of the study analyzes the 2006 Lebanon War, beginning with the Hezbollah ambush of an Israeli patrol, which formed the pretext for an Israeli invasion of southern Lebanon. The short war that followed highlights the complexity and further changes in irregular warfare, to the extent that some observers have called it a classic example of "hybrid-war."[541] Both phases of the Israeli-Hezbollah conflict feature different aspects of irregular warfare and a comparison of the two reveals a strong contrast between classic guerrilla warfare and terrorism, and network-style warfare.

B. LEBANON OVERVIEW

The idyllic scenery provided by Lebanon's position on the Mediterranean coast belies its recent chaotic history, and the devastation it has seen in the last 30 years. Until the brutal civil war, which turned its capital, Beirut, into a devastated war zone, it was a popular vacation destination, with tourists enjoying the combination of coastline and scenic mountains. It is bordered by Syria to the north and east, the Mediterranean Sea to

[540] Norton, *Hezbollah*, 38.

[541] Hoffman, *Conflict in the 21st Century*, 35.

the west and Israel to the south, along a 79-kilometer border. Most of Lebanon is fairly rough terrain, with rolling hills and rugged mountains, with the exception of the Beqaa Valley to the northeast.

Figure 13. Lebanon and the Northern Levant Region[542]

Centuries of trade and migration shaped Lebanon, and contributed to its mosaic of cultural diversity. Its physical terrain has helped isolate, protect, and generate numerous factions based on religion, ethnic, and clan differences. Ethnically, it is 95% Arab, with a Muslim majority of 59.7% (Shi'a, Sunni, and Druze) and 39% Christian (primarily Maronite, Greek Orthodox and Greek Catholic), with over 17 different religious sects

[542] University of Texas at Austin, University of Texas Libraries, Perry–Castañeda Library Map Collection, Lebanon Maps, http://www.lib.utexas.edu/maps/lebanon.html.

recognized.[543] The Shi'a sect is the majority sect along the Israeli border area, although it also occupies a large area in the northeast, including much of the Beqaa Valley. Lebanon is truly a complex, jigsaw of different ideologies, ethnic groups, political factions, and armed organizations.

Likewise, brutal invasions and internal conflict have also played a powerful role in forming and shaping this diversity. While most modern accounts reflect on the prosperity prior to the Lebanese Civil War in the mid 1970s, internal conflict and external influence in WWI and WWII, and the political struggles following independence, left Lebanon with a shaken sense of normalcy.[544] Its establishment as a modern, independent state following the departure of Vichy French colonial occupation in November 1943 was based on a power-sharing arrangement between each of the three major religious sects.[545] This system managed to maintain stability until increasingly violent internecine struggles exposed the many, sharp divisions in the country. The Arab-Israeli conflict exacerbated these struggles. The Arab-Israeli wars, most notably the 1967 war, forced an immigration of Palestinian refugees into southern Lebanon, where they formed militias to attack Israel. The Jordanian expulsion of thousands of armed guerrillas following the Jordanian civil war in 1970–71 led to the movement of the PLO into southern Lebanon, where it was able to control much of the region, and play a role in the outbreak of civil war in 1975.[546]

These divisions are reflective of regional complexity and differences and have invited numerous state and non-state actors' participation inside Lebanon. Such participation has largely shaped what modern Lebanon is today, and continues to fuel its internal and external struggles. Both Syria and Iran have been deeply involved in Lebanon. Iranian influence grew dramatically following the Ayatollah Khomeini's 1979 Islamic Revolution. Each of these states sponsors various groups and interests within

---

[543] Data from The World Factbook, https://www.cia.gov/library/publications/the-world-factbook/geos/le.html.

[544] Charles Winslow, *Lebanon: War and Politics in a Fragmented Society* (New York: Routledge, 1996), 1.

[545] Helena Cobban, *The Making of Modern Lebanon* (Boulder, CO: Westview Press, 1985), 46.

[546] Norton, *Hezbollah*, 14.

Lebanon and uses them to further their interests. Israel's involvement follows much the same pattern by backing numerous political and militia groups over the years and uses them to further their national security interests.

C. HEZBOLLAH BACKGROUND

Hezbollah arose in 1982 after the Israeli invasion in June to force the PLO and other Palestinian militants out of southern Lebanon. Its initial beginnings may be traced to several factors and events, but the civil war, which began in 1975, was a major precipitating event. This internal conflict may have resulted from increased pressure caused by the Arab-Israeli conflict and the rise of active Palestinian militant groups, and it fragmented Lebanon at its socio-cultural fault lines. The Palestinian resistance movement directly challenged Lebanon's elites, while various ethnic and political groups formed numerous militia groups to assert their identity and hold on power. Notable among these groups was Amal (*Afwaj al-Muqawama al-Lubnaniya*, or Lebanese Resistance Detachments), a Shi'a resistance group that joined a coalition opposed to Maronite control, and which surged in power following the Israeli invasion of Lebanon in 1978 and the Iranian revolution of 1978–79.[547] As Amal tacitly supported Israel in its efforts to destroy the PLO, was backed by the Syrian government, and expanded into a larger political movement, a small cadre of its members began to oppose Amal's de facto secularism and hold on power. These members were young Shi'a leaders, trained in the Iraqi seminaries of Najaf and Karbala, who viewed themselves as revolutionaries in the Iranian mode, and sought to develop an Islamic style of rule.[548]

Iran, for its part, viewed Amal and the emerging political structures in Lebanon as a pro-Western influence, and aimed to counter its rise. In late 1982, Iran sent several hundred members of its Iranian Revolutionary Guards Corps (IRGC), also known as the *Pasdaran* to Lebanon to support the newly formed Shi'a organization.[549] The IRGC was

[547] Norton, *Hezbollah*, 22.

[548] Jamal Sankari, *Fadallah: The Making of a Radical Shi'ite Leader* (London: Sadi, 2005), 172.

[549] Shimon Shapira, "The Origins of Hezbollah," *The Jerusalem Quarterly* 46 (1988): 22; Harik, *Hezbollah*, 40.

familiar with Lebanon, as many of its senior members had trained with the PLO in the Beqaa Valley, prior to Khomeini's return to Iran.[550] The arrival of these trainers and full Iranian support initiated efforts that catalyzed the movement, provided resources, and supplied a full-fledged ideological purpose. This purpose drew other Shi'a leaders who favored an Islamic state, including Abbas Musawi, Amal's second-in-command, who brought additional fighters and resources to the Beqaa valley. Islamic fervor took root in the town of Baalbeck, and it became a revolutionary nursery filled with an "Iranian" atmosphere.[551] Syria also provided support to maintain its alliance with Iran, keep its Lebanese ally, Amal, in-check, and gain a means for striking at both Israel and the United States, but it has been motivated more by convenience than common cause.[552]

Ideologically, Hezbollah closely follows the Iranian line, as evidenced by its "founding" document of 1985, which is in the form of a letter addressed to the "Downtrodden in Lebanon and in the World." This letter cites the Iranian revolution as a model for action and anticipates the possibility of an Islamically-motivated revolution. While the Iranian revolution produced a demonstration effect throughout the Middle East, it was felt most strongly amongst the Lebanese Shi'a.[553] Still, replacing the Lebanese government was never the main focus, despite its corruption and use as a scapegoat. Instead, the Hezbollah leadership focused on a sacred obligation to conduct violent jihad against those who had occupied Muslim lands—the Israelis, whom they viewed as the primary cause of the suffering of the Muslims in Lebanon. Beyond Israel, the United States was viewed as the main enemy, and in their opening letter, Hezbollah's founders

---

[550] Norton, *Hezbollah*, 32.

[551] Shapira, "The Origins of Hezbollah," 123.

[552] Norton, *Hezbollah*, 35.

[553] The term "demonstration effect" describes the occurrence whereby a revolutionary action in one place may serve as a catalyst for a similar event in another place. The degree to which this is possible depends on many factors, including cultural similarities and similar opportunities. The clearest recent example is the social unrest sparked by events in Tunisia, and now spreading through several other Middle Eastern countries. For further detail, see Thomas H. Greene, *Comparative Revolutionary Movements* (Englewood Cliffs, NJ: Prentice Hall, 1984), 173–174.

stated, “Imam Khomeini, the leader has repeatedly stressed that America is the reason for all our catastrophes and the source of all malice. By fighting it, we are only exercising our legitimate right to defend our Islam and the dignity of our nation.”[554]

Hezbollah draws considerable strength from a cohesive social network among the Lebanese Shi’a, as well as a globally dispersed network of supporters, all of who are united in a common ideology. This strong base of support originated in the Baalbeck region, as Nisar Hamzeh describes, “…the makeup of the local population, totally Shi’ite and organized along kinship networks, was extremely advantageous for recruitment, information, and refuge. As a matter of fact, the vast majority of Hezbullah’s leaders came from the towns and cities of Baalbeck-Hirmil.”[555] It expanded this initial base to the southern suburbs of Beirut, and since the initial launching of its resistance activities, to diaspora elements throughout the globe.

D. SOUTH LEBANON CONFLICT: 1982–2000

Israel’s invasion of Lebanon on June 6, 1982, code-named Operation Peace for Galilee, ended an 11-month ceasefire with the PLO, which renewed hostilities originally started when Israel launched Operation Litani in 1978 to create a buffer zone in southern Lebanon.[556] While the attack was largely in response to the Abu Nidal faction of the PLO and its assassination attempt against Israeli’s ambassador to the United Kingdom (UK), Shlomo Argov, its main purpose was to secure a buffer zone in South Lebanon. The Israelis invaded with heavy divisions and air strikes in a three-pronged advance, including an amphibious landing that pushed all the way to Beirut, trapping and killing numerous PLO elements. This blitzkrieg-style assault, using six divisions and air force support, seized more than a third of the country and fought against irregular PLO forces,

[554] Augustus Richard Norton, *Amal and the Shi’a: Struggle for the Soul of Lebanon* (Austin, TX: University of Texas Press, 1987), 170.

[555] Ahmad Nizar Hamzeh, *In the Path of Hizbullah* (Syracuse, NY: Syracuse University Press, 2004), 88.

[556] Norton, *Hezbollah*, 32.

as well as Syrian regular forces, including armor.[557] Militarily, this assault was highly successful. Both a guerrilla force and conventional Syrian units were defeated in simultaneous action over three weeks. Of note, in some urban areas, PLO guerrillas stood and fought against overwhelming odds and displayed a remarkable tenacity.[558] While it successfully forced the PLO to withdraw, the Israeli invasion provided a galvanizing effect on the Shi'a revolutionaries and aided in their transformation from a loosely affiliated cabal of like interests into a recognizable organization.[559] As former Israeli Prime Minister Ehud Barak stated, "when we entered Lebanon…there was no Hezbollah. We were accepted with perfumed rice and flowers by the Shia in the south. It was our presence there that created Hezbollah."[560] Little doubt exists that the Israeli invaders provided a more compelling enemy than the infighting, which had characterized the Lebanese civil war. Moreover, with the expulsion of the PLO, Hezbollah was really the only Lebanese militia movement able to step in and represent the Shi'a against the Israeli invader and its Lebanese proxy-force, the South Lebanese Army (SLA). As the situation deteriorated, and warring factions continued to attack each other, the United States, France, and Italy deployed peacekeepers as part of a Multi-National Force (MNF) to facilitate demobilization and the departure of the PLO.

Hezbollah fought back, launching numerous guerrilla attacks against the MNF and Israeli forces, and spearheading the efforts of other militias as well. The first notable attack was a suicide attack against the seven-story Israeli military headquarters in Tyre, on November 11, 1982, which resulted in 91 Israelis killed.[561] This attack represented the first significant Hezbollah terrorist strike against Israel Defense Forces (IDF) forces, but

---

[557] Trevor N. Dupuy and Paul Martell, *Flawed Victory: The Arab-Israeli Conflict and the 1982 War in Lebanon* (Fairfax, VA: Hero Books, 1986), 92.

[558] Joe Stork and Jim Paul, "The War in Lebanon," from *MERIP Reports, No. 108/109, The Lebanon War* (Middle East Research and Information Project, September–October 1982), 3, http://www.jstor.org/stable/3012233.

[559] An indication of just how loose the initial elements of what would become Hezbollah were is observed in Dupuy and Martell, *Flawed Victory*, 197–199, where they list the various Lebanese elements vying for power following the 1983 ceasefire agreement. Hezbollah is not listed, but the Islamic Jihad is discussed as a group of "fanatic members" of the Amal.

[560] Ehud Barak, *Newsweek*, July 18, 2006, as cited in Norton, *Hezbollah*, 33.

[561] Hamzeh, *In the Path of Hizbullah*, 81–82.

many more would follow. The significant destruction and the embarrassment of the bombing was such that Israeli would not admit it was a suicide bombing.[562] Such attacks made international headlines with the April 18, 1983 suicide bombing of the U.S. Embassy in Beirut, which killed 63 people and was claimed by the Islamic Jihad organization.[563] This attack was followed by another suicide bombing on October 23, 1983, which destroyed the U.S. Marine headquarters compound, killing 241 Marines and wounding 100. Almost simultaneously, another truck laden with explosives smashed into the French peacekeeping compound, resulting in 150 casualties.[564] Just days later, another suicide bombing targeted Israeli forces in headquarters outside of Tyre, killing 28 Israeli military and security personnel and 32 Lebanese and Palestinian detainees.[565] By 1985, the IDF had withdrawn back into southern Lebanon and established a security zone covering 10% of Lebanon. This security zone was fortified with company-sized outposts manned by the IDF and SLA forces.[566] Hezbollah sought to continue the offensive against the IDF and its Lebanese allies, attacking asymmetrically with the goal of "confusing the enemy and obliging its command to call for a constant state of alert, eventually leading to the exhaustion and decline in power."[567] This offensive slowly eroded Israeli public support for the war, compounding the frustration felt by the IDF, who were challenged with such an aggressive guerrilla force. A steady stream of suicide bombings, devastating ambushes and indirect rocket attacks represented offensive action designed to force an Israeli withdrawal.

---

[562] Multiple witnesses to this attack claim to have seen a Peugeot speeding to the building, as well as a monument near Baalbek dedicated to Ahmad Qassir, the suicide bomber who executed the attack. The attack remained unclaimed for a variety of reasons, but mostly to protect those responsible on both sides. For more on this attack see, Ronen Bergman, *The Secret War with Iran* (New York: Simon & Schuster, 2008), 65; Hamzeh, *In the Path of Hizbullah*, 81–82.

[563] Dupuy and Martell, *Flawed Victory*, 200.

[564] Ibid., 206.

[565] Ibid., 207.

[566] Matt Matthews, *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War* (Fort Leavenworth, KS: Combat Studies Institute Press, 2008), 7.

[567] Sheikh Naim Qassem, *Hizbullah: The Story From Within*, trans. Dalia Khalil (London, Saqi, 2005), 71.

In 1993, Israel launched Operation Accountability, a massive air and artillery campaign in response to increased Hezbollah action. This operation was largely a standoff attack relying on the Israeli Air Force (IAF) and long-range artillery to strike suspected Hezbollah positions. The next major clash occurred in 1996, when Israeli initiated Operation Grapes of Wrath, in response to Hezbollah rockets wounding 38 civilians in northern Israel.[568] This operation again relied mostly on air and long-range artillery using precision fire against a vast array of targets. The Israeli bombardment targeted Hezbollah positions, but also placed a significant emphasis on civilian infrastructure targets and civilian population centers in southern Lebanon. The purpose of these attacks was to force Lebanese civilians from the area and to compel Lebanese and Syrian governments to act against Hezbollah. Israeli airpower demolished significant portions of the Lebanese infrastructure, warning the government that further inactivity towards Hezbollah would lead to wider destruction.[569] However, an impressive government humanitarian and reconstruction response to the damage, as well the regional and global condemnation over the Israeli shelling of the United Nations (UN) base at Qana, which killed 98 and wounded 101 Lebanese civilians, mitigated any positive effects Israel hoped to achieve.[570] Most significantly, while Hezbollah suffered some losses, its military operations remained largely unaffected. Throughout the bombings, Hezbollah struck back at Israeli with hundreds of Katyusha rockets and forced Israelis in the north into bomb shelters. Despite a tacit Hezbollah-Israeli agreement not to target civilians, the war in southern Lebanon continued and the IDF continued to take losses. A growing public dissatisfaction with the effort led to calls for a withdrawal, and in 1999, newly elected Israeli Prime Minister Ehud Barak promised Israel that he would withdraw the IDF from southern Lebanon within 12 months.[571] As Israeli units began transitioning to withdrawal, they moved into a series of 50 fortified positions, 42 of which were

[568] Matthews, *We Were Caught Unprepared*, 9.

[569] Harik, *Hezbollah*, 117.

[570] Ibid.

[571] Norton, *Hezbollah*, 88.

manned primarily by the SLA.[572] Hezbollah continued devastating attacks, using modern weapons, such as TOW missiles, to inflict losses despite the fortified positions. With Barak's announcement of withdrawal, the badly shaken SLA began to evacuate its positions, completely disintegrating in the face of Hezbollah's onslaught. Eyewitness reports stated, "Israeli troops staggered back across the border, telling reporters that their military equipment and training had proven useless against Hezbollah, and its Lebanese allies."[573] The planned withdrawal turned into a rout, with Israeli and SLA forces literally stampeding back across friendly lines.

1. Israeli Invasion and Occupation

The Israeli military organization was based on a traditional military hierarchy during their 1982 invasion, and subsequent occupation of southern Lebanon. Israeli's military is organized and structured similar to most modern Western armies. Its initial assault into Lebanon and the advance to Beirut consisted of combined arms with intensive air support, gained by air supremacy established in the first day of the war. The invading forces, totaling 76,000 IDF troops, were organized into division-sized task forces, called *ugdah*. These task forces were organized in a traditional manner and combined different infantry and armored units based on their proposed tasks and area of operations.[574] Following the invasion, most of the IDF withdrew, and by mid-summer of 1983, there were 15,000 Israeli occupying forces. These forces were responsible for controlling nearly 2,800 square kilometers inhabited by a population of over 5000,000, composed of Shiite and Sunni Muslims, Christians, Druze, and Palestinians.[575] It was this force, flush with its recent victory, which established fortified outposts throughout the occupied sector. Company-size units manned these outposts, assigned to strongpoint key areas throughout a designated sector.

---

[572] Matthews, *We Were Caught Unprepared*, 10.

[573] Joel Himelfarb, "Hezbollah's Deadly Record," *The Washington Times*, March 16, 2005, as quoted in Matthews, *We Were Caught Unprepared*, 11.

[574] Dupuy and Martell, *Flawed Victory*, 92.

[575] Ibid., 200.

Israeli military doctrine generated over its early wars placed an emphasis on, "speed, daring, and deep penetrations without regard to flank security….fire support was to be provided by ground attack aircraft to maintain the pace of advance."[576] These areas of emphasis were battle tested by one of the most combat-proven modern militaries, with an unparalleled record in multiple wars over the last half century. Many of the lessons that formed Israeli doctrine were based on the successes in the Yom Kippur War of 1973, primarily the simultaneous use of combined arms in a fluid manner. The intelligence function, to support such rapid operations, is viewed with equal emphasis, and given parity with operational commands and efforts. However, this doctrine, displayed so vividly in the initial invasion, provided little basis for an occupying force faced with a growing irregular opponent.

The operational methods employed during the initial invasion stressed synchronized maneuver, close coordination between a ground unit's advance and air support, bypassing areas of resistance where possible and using aerial bombing in areas where it could be employed, including several Palestinian refugee camps. These methods were largely successful against PLO and Lebanese forces that fought in a fairly conventional manner, notwithstanding their organization into smaller guerrilla units. During the following occupation, Israeli operational methods became much more static, based largely on securing a framework of outposts, and less on proactive attempts to dismantle a growing Hezbollah threat.

The core of the Israeli information strategy was simply providing a justification for the invasion against the PLO, which used the attempted assassination against Argov as a pretext for intervention. Beyond this, little information strategy was employed, other than to portray the PLO as terrorist aggressors who continued to threaten security in Israel. Information operations during the initial invasion consisted largely of the use of propaganda and early-warning leaflets, which informed civilians of impending bombings. At the tactical level, Israeli forces strictly controlled journalists and media access.

[576] Stephen Biddle, "Land Warfare: Theory and Practice," *in Strategy in the Contemporary World: An Introduction to Strategic Studies*, ed. James Wirtz, Eliot Cohen and John Baylis (Oxford, UK: Oxford University Press, 2002), 540–541.

However, despite their best attempts, the siege of Beirut became a divisive affair, as the images of civilian casualties and horrific destruction resulting from the fighting in a densely civilian-occupied area were broadcast to the world. These images led to a growing dissatisfaction among the Israeli public, and even field commanders resigned rather than participate in any advance into Beirut.[577] By that point, the main elements of the initial information strategy had worn out, which were replaced with growing condemnation over the destruction. As the occupation continued, overall support continued to drop, and the Israelis lacked an information strategy that could successfully counter Hezbollah's growing image.

2. Hezbollah's Irregular Response

Initially operating as an independent irregular force, separate from the Lebanese government, Hezbollah began regularly attacking Israeli and SLA forces. These attacks were largely classic guerrilla actions, and also incorporated "terrorist" actions, such as the use of suicide bombings—aimed primarily at IDF forces. At the same time, Hezbollah was also asserting itself against other Lebanese militias and fighting for increased control against Amal and other Lebanese confessional groups, most notably the Maronites. Even after the Taif Agreement on a national reconciliation, Hezbollah maintained its arms, using the Israeli presence in South Lebanon as justification, which kept its "…military capabilities intact after the end of the civil war in 1990, when all of the other paramilitary groups were forced to disarm. This left them as the predominant actor in South Lebanon…."[578]

Organizationally, Hezbollah's original formal structure was fairly centralized and hierarchical, but operationally and at the local level, a high degree of connectivity existed, which was facilitated by local tribe and village connections. Organizational connectivity, the overarching purpose, was based primarily on ideology, even more than kinship—as evidenced by other Lebanese Shiites loyalty to more moderate groups, such

[577] Daniel I. Helmer, *Flipside of the COIN: Israel's Lebanese Incursion Between 1982-2000* (Fort Leavenworth, KS: Combat Studies Institute Press, 2006), 43.

[578] Tom P. Najem, "Palestinian-Israeli Conflict and South Lebanon," *Economic and Political Weekly* 35, no. 46 (November 11–17, 2000): 4007, http://www.jstor.org/stable/4409949.

as Amal. This purpose provided cohesion and unity between a larger network at the level of the "masses," and an elite leadership group heading the formal structure. The ideological unity allowed Hezbollah to adapt itself organizationally; thus displaying a great deal of flexibility, and allowing for a broad range of functions within the organization. As Mona Harb states, this results "because they operate as an integrated and holistic network. This network produces individual and collective meaning to its beneficiaries, which in turn, explains how and why Hizballah is legitimized as a dominant order among Lebanese Shi'a."[579] Structurally, the organization features collective leadership. A seven-member *Majlis Shura* council is composed of six clerics and one lay member, led by Secretary-General Hassan Nasrallah as the senior cleric.[580] This body is nominally elected, but its elite membership is tightly controlled, and resembles more of an appointment by select influential members and the Central Council than any open election.[581] The management of the organization is delegated to an administration apparatus, the *Shura Tanfiz*, which oversees five councils, the Executive Council, the Politburo, the Parliamentary Council, the Judicial Council, and the Jihad Council. Each of these councils oversees most of the parties' business. The Executive Council runs the day-to-day social outreach and interaction programs. The military and security apparatus of the organization are separate and surrounded with a great deal of secrecy, but it appears that there are two main elements, the Islamic Resistance (*al-Muqawamah al-Islamiyah*) and the Party Security (*Amn al-Hizb*), both of which report to, and closely coordinate with, the party's Shura Council.[582] The Islamic Resistance was Hezbollah's original paramilitary organization, and the covert nature of membership in these organizations reveals Hezbollah's ability to manage both an overt political party, as well as its original resistance activities.

---

[579] Mona Harb and Reinoud Leenders, "Know Thy Enemy: Hizbullah, 'Terrorism' and the Politics of Perception," *Third World Quarterly* 26, no. 1 (2005): 187, http://www.jstor.org/stable/3993770.

[580] Reflective of the high levels of interaction and consensus building among tribal forms of organization, Hassan Nasrallah also sits on three of the other councils and provides a level of interaction and a high degree of connectivity usually not present in classic hierarchical structures.

[581] Hamzeh, *In the Path of Hizbullah*, 47.

[582] Ibid., 44–70.

Much of Hezbollah's doctrine resembled classic guerrilla warfare, but they applied it in a relentless manner, which demonstrated an increasing capability for devastating swarming. Beginning in 1985, it aggressively attacked IDF and SLA outposts throughout the security zone, basing its actions on a set of principles formulated to "defeat a relatively fixed, technologically advanced enemy."[583] These irregular warfare tenets provide a doctrinal blueprint for Hezbollah's actions:

1. Avoid the strong, attack the weak—attack and withdrawal!
2. Protecting our fighters is more important than causing enemy casualties!
3. Strike only when success is assured!
4. Surprise is essential to success. If you are spotted, you have failed!
5. Don't get into a set-piece battle. Slip away like smoke, before the enemy can drive home his advantage!
6. Attaining the goal demands patience, in order to discover the enemy's weak points!
7. Keep moving; avoid formations of a front-line!
8. Keep the enemy on constant alert, at the front and in the rear!
9. The road to the great victory passes through thousands of small victories!
10. Keep up the morale of the fighters; avoid notions of the enemy's superiority!
11. The media has innumerable guns whose hits are like bullets. Use them in the battle!
12. The population is a treasure—nurture it!
13. Hurt the enemy and then stop before he abandons restraint![584]

These principles provide a concise summary of Hezbollah's guerrilla operations, as well as reveal an insightful understanding of irregular warfare. In addition to publishing such principles, one of Hezbollah's earliest, and continued, strengths was the disciplined focus of its members, which is clearly evident in the nature of its operational activity. The emphasis on martyrdom operations, extolled in the Iranian-influenced jihadist ideology,

[583] Matthews, *We Were Caught Unprepared*, 7.

[584] Ehud Ya'ari, "Hizballah: 13 Principles of Warfare," *The Jerusalem Report*, March 21, 1996, quoted in Helmer, *Flipside of the COIN*, 53–54.

provides a purpose and motivation that confounds the argument that guerrilla warfare "…is not for innocent youth motivated primarily by romantic idealism but for seasoned veterans whose living conditions are constantly in flux."[585] The combination of lessons learned during the 1982–2000 conflict, and the growing connectivity and consolidation of the organization, provided the elements that would generate into an effective fighting network.

Operationally, Hezbollah focused mainly on the primary methods of guerrilla warfare—the raid and the ambush. One of the more notable ambushes occurred in September 1998, when 12 Israeli naval commandos from the elite unit, *Sayyit*, were decimated outside the Insariyyah village in South Lebanon.[586] Hezbollah's growing ability to fight IDF forces was further displayed in the killing of a paratroop unit commander and three of his lieutenants, during an Israeli raid into the Beqaa Valley in February 1999.[587] In addition, it established the use of suicide bombings as a key aspect of its operations, utilizing the principles behind a raid, but achieving devastating effects in a "stand-off" manner, thereby eliminating the hardest aspect of raid planning—withdrawal.

Hezbollah Martyr (Suicide) Operations				
Group Name	*Target*	*Location*	*Casualties*	*Date*
Hezbollah	Israeli Military HQ	Tyre	90 Israelis killed	November 1982
Islamic Jihad	U.S. Embassy	Ras-Beirut	80 killed	April 1983
Islamic Jihad	U.S. Marine HQ	Beirut	241 U.S. killed	October 1983
Hezbollah	French Military HQ	Beirut	80 French killed	October 1983
Hezbollah	Israeli Military HQ	Tyre	29 killed, 30 injured	October 1983
Hezbollah	IDF command post	Khiam	12 killed, 14 injured	March 1985
Hezbollah	IDF motorcade	Tal-Nhas	25 killed, 11 injured	August 1988

[585] Greene, *Comparative Revolutionary Movements*, 136.

[586] Hamzeh, *In the Path of Hizbullah*, 90.

[587] Ibid., 92.

Hezbollah Martyr (Suicide) Operations				
Hezbollah	Motorcade	Qliy'a	25 killed and injured	August 1989
Hezbollah	Infantry Patrol	Al-Jarmaq	9 killed and injured	April 1995
Hezbollah	Command Post	Rab-Thalathin	None	March 1996
Hezbollah	Military Camp	Marja'youn	None	December 1999

Figure 14. Hezbollah Suicide Operations Against International and IDF Targets, 1982–1999[588]

Buttressing these higher profile martyrdom attacks was a constant use of explosive ambushes, which grew in sophistication over the years. IDF forces attempting to travel throughout the region were subject to constant IED attacks, and in March of 1999, a powerful explosive device killed Brigadier General Erez Gerstein, the head of the IDF's liaison unit in South Lebanon, and three others.[589] This attack was a tremendous setback for Israeli operations, and may have been the final shock for an Israeli public weary of the occupation. Of note, although its field and operation security is robust, Hezbollah is fairly overt about displaying its military formations, and groups of up to 5,000 have been reported on parade.[590]

Hezbollah's use of information strategy, emphasized from its founding, grew in sophistication during the period of occupation. Initially visible in publically released statements following attacks, Hezbollah's information campaign grew to include multiple newspapers, journals, radio stations, and even its own television broadcasting station. By 1988, Hezbollah had three radio stations, and it latest one, Al-Nour, is one of the leading professional radio stations in the Middle East. Television broadcasting is perhaps the most visible and most influential aspect of Hezbollah's information architecture, and its sophistication continues to grow since the founding of its Al-Manar ("lighthouse")

[588] Data from similar tables researched and compiled from various Lebanese sources and Ahmad al-Musawi, "Shahada wa-istishhadiyyin," *Al-Shira'a*, June 5, 2000, 33–34, by Hamzeh, *In the Path of Hizbullah*, 81–82.

[589] Hamzeh, *In the Path of Hizbullah*, 92.

[590] Bergman, *The Secret War with Iran*, 87.

channel in 1991.[591] Its primary audience is the Shi'a population of southern Lebanon, and it portrays a mix of jihadist ideology with news, political commentaries, and announcements. It also is notable for being the first, and only, place where the Arab and Muslim have seen Israeli soldiers killed and dying at the hands of the Islamic resistance. These images turned the feeling of a defeat following the Israeli invasion into a growing sense of victory, especially following the Israeli withdrawal, and generated a considerable following throughout the region.[592] Hasan Nasrallah describes the role of media in asymmetric conflict:

> The relationship between the media and the resistance, I can assure you from experience is very strong and close. It is said that the media aspects represent half of the battle, or three quarters or two thirds. These calculations are inaccurate, but without doubt the media are one of the most important weapons of combat and resistance; it has considerable effects on the enemy, on allies, and the morale of the resistance. We lived this experience ourselves and found that, in certain cases, the media performance affects the cause of the battle, the course of the confrontation….[593]

An indicator of the growing effectiveness of Hezbollah's use of information is its propaganda coup achievement following the Insariyyah ambush. Images and press releases about the elimination of a team from one of Israel's most elite units provided a considerable boost to Hezbollah forces, while sowing further doubt among the Israeli population. Since 1996, Hezbollah has had an official organization website that provides current news, updates from leadership and resistance advice.

---

[591] Rid and Hecker, *War 2.0*, 149.

[592] Hamzeh, *In the Path of Hizbullah*, 59.

[593] Rid and Hecker, *War 2.0*, 153.

1st Israel-Hezbollah War				
	Organization	Doctrine	Operations	Information Strategy
Israeli Forces	*Traditional Hierarchy *Unity of Command	*Combined Arms *Synchronized Maneuver *Sector security	*Counter-guerrilla Operations *Fixed outposts	*Basic Propaganda *Enemy Focused
Hezbollah Forces	*Formal leadership structure *Numerous cells *Highly connected	*Swarming *Offensive Attacks *"Terror" Strikes against IDF	*Capable Small Unit Tactics *Suicide Operatives	*Sophisticated Media Apparatus *Constant Engagement

Table 8. Evaluation of the 1st Israel-Hezbollah War

3. Analysis of Counter-Network Framework

Much like the initial Russian efforts in the 1st Russo-Chechen war, it is difficult to discern much application of any of the principal variables comprising the requirements for effective counter-network operations. Still, their absence and the events of the case study provide some grounds for inference, if not causal explanation.

a. Offensive Swarming

The Israeli offensive in 1982 was a full-scale maneuver operation involving traditional combined-arms doctrine. Much of the efforts that followed, up through and including the withdrawal in 2000, were aimed at holding terrain and maintaining a buffer zone. While elite units attempted raids against Hezbollah targets, these were largely ineffective and the devastating ambushes against some of them reveal a lack of surprise. Israeli actions taken against Hezbollah were largely aimed at their leadership structure, much like similar actions taken against the PLO. However, these actions rarely succeeded, largely because intelligence about the organization was difficult to gain, and also because Israeli operations were focused on sustaining their role as a

"peacekeeping" force, however embattled. What few operations that did succeed had little effect against the growing network. The medium-sized operational sweeps (Operation Accountability in 1993 and Operation Grapes of Wrath in 1996) were largely conventional cordon and search campaigns, and Hezbollah fighters flowed right back into the areas as soon as the IDF vacated them. For most of the time, Israeli forces occupied southern Lebanon and focused on simply securing the northern border area. Some efforts were directed towards focused targeting, but they generated little significant operational tempo, and occurred later in the war. As Thomas Henricksen reports, "to counter the growing battlefield skills of the Islamic Resistance, the IDF turned to unique units such as *Sayeret Egoz* that conducted aggressive patrolling and ambushing of insurgents. These units were effective but not on a decisive scale."[594] Further, targeted killings, such as the notable assassination of Hezbollah's Secretary-General Abbas Musawi in 1992, brought additional Hezbollah rocketing of the northern Galilee, further weakening Israeli public support.

b. Illumination

Israeli efforts at illumination focused primarily on generating operational activity and then reacting to it. Many of the Israeli operations were aimed at disrupting Hezbollah's ability to launch rockets against the northern settlements, and were more terrain- and capability-based than focused against Hezbollah as an organization. Still, efforts to collect intelligence against Hezbollah existed, but were rather limited in scope. At the end of 1989, the Israeli intelligence organization, Shin Bet, established the Mabat. This SLA organization was designed to be a network of intelligence collectors able to report to both SLA and IDF forces, but its lack of local connections and poor capabilities resulted in little gains.[595] For the most part, attempts at infiltrating the Hezbollah organization were frustrated by a robust security apparatus, and it was clear that Hezbollah's growing sophisticating was a stark contrast to the complacent, centralized,

[594] Thomas H. Henriksen, *The Israeli Approach to Irregular Warfare and Implications for the United States*, JSOU Report 07-3 (Hurlburt Field, FL: The Joint Special Operations University Press, 2007), 33.

[595] Bergman, *The Secret War with Iran*, 83.

and fairly corrupt PLO.[596] Moreover, Israeli intelligence was generally more concerned with force protection, and preventing security-zone outposts from being overrun. Despite Israel's reputation for effective HUMINT, it found itself largely at a loss in trying to penetrate Hezbollah. In addition, Hezbollah's disciplined approach and sophisticated counter-intelligence training frustrated most efforts at exploitation.[597]

c. Information Disruption

In stark contrast to Hezbollah's growing use of information and a sophisticated strategy employing mass media, Israeli counter-efforts demonstrated little success. Clearly, Hezbollah's deeply rooted Shi'a jihadist mindset was difficult to counter, and even Lebanese moderate groups opposed Israeli intervention and presence. Israeli efforts during the invasion were focused almost entirely against PLO forces, and as the war progressed into its occupation phase, Israel never fully pursued efforts to attack Hezbollah's information strategy.

d. Fusion

Although recent Israeli efforts seem to emphasize both organizational and doctrinal fusion, these developments were not evident prior to 2000. It is unclear if such capabilities would have provided much assistance without the strategy to utilize them, especially since Israel only actively sought to target Hezbollah when it had already lost most of the initiative.

In the end, an irregular opponent whose asymmetric tactics revealed Israeli errors in strategy, and perhaps an unwillingness to change its tried-and-true approach to warfare, brought Israel, a country that had achieved success in four consecutive military victories in 1948, 1956, 1967, and 1973, low.[598] Israel's lightning success in the conventional invasion resulted in a reliance on a traditional approach to

---

[596] Yezid Sayigh, "Israel's Military Performance in Lebanon, June 1982," *Journal of Palestine Studies* 13, no. 1 (1983): 25–27, http://www.jstor.org/stable/2536925.

[597] Bergman, *The Secret War with Iran*, 85.

[598] Helmer, *Flipside of the COIN*, 83.

securing a security zone in southern Lebanon. The flaws in this traditional approach were increasingly revealed as Hezbollah developed its strategy to force the Israelis into a strategic dilemma; a strategy made possible by increasingly sophisticated irregular warfare and terrorist attacks. Ultimately, neither Israel nor its SLA allies were able to bring Hezbollah into any kind of significant engagement, and the overall casualty ratio was nearly 1:1, with Israel and the SLA losing 1,250 to Hezbollah's 1,248.[599] The final ceasefire established a border zone, and a "Blue Line" of demarcation on June 7, 2000 that was over watched by UN peacekeeping forces.

E. GLOBAL TERROR ATTACKS

In addition to guerrilla attacks against IDF forces, Hezbollah was responsible for, or complicit in, a host of significant "terrorist" attacks. The primary focus of these attacks was against Israeli forces, and in many ways, they could be considered "battlefield" actions against an occupying military force. Others are clearly terrorist attacks, focused beyond Israeli forces, attacking U.S. and international peacekeepers inside Lebanon, and other designated targets around the globe. In addition to the bombing in Beirut, in July 1994, Hezbollah added a new tactic to its arsenal, terrorist attacks against Israeli interests worldwide. Truck bombs that targeted Israeli and Jewish targets in both Buenos Aires and London showed the global reach of the terrorist organization, and became a significant weapon with which to counter-balance Israeli targeting.[600]

These terror attacks are significant because they demonstrate a level of global connectivity and networking that cannot be countered in a classic irregular warfare setting, such as seen in a COIN doctrine and historical efforts. Hezbollah's international terror campaign paved the way for similar approaches by other irregular networks, whether insurgents or global terrorists.

---

[599] Hamzeh, *In the Path of Hizbullah*, 94.

[600] *Flipside of the COIN*, 57.

F. THE 2006 CONFLICT

By 2006, Hezbollah had transformed itself from just a radical militia and terrorist organization into a full-fledged mainstream political party. Its overall success on the battlefield helped in this transformation as well, as the Lebanese realized that without Hezbollah's capability, no one else could resist Israeli aggression. This transformation actually began as early as 1990, when Hezbollah began making plans to field candidates for upcoming elections, and with the evacuation of the SLA and Israelis from southern Lebanon, it rapidly consolidated physical control.[601] As Lebanon slowly rebuilt during the first five years of the decade, Hezbollah continued to gain more support, achieving electoral success, winning 14 parliamentary seats, and holding two cabinet posts in the Lebanese government by 2005.[602] Overall, the interlude between wars brought an increasing number of tourists back to Beirut and Lebanon, and it had recovered its status as a high-end vacation destination. At the same time, Hezbollah reach out to other Lebanese parties, building a framework for increasing political control that brought stability back to southern Lebanon.

Despite the peaceful outlook, tensions were growing between Hezbollah and Israel, and the "rules of the game," that had allowed for a moderate level of tit-for-tat violence, were slowly being ignored.[603] Intercepted communications between Hezbollah and Hamas, an attempted Hezbollah kidnapping in November 2005, and increasing levels of retaliation all pointed to an increased probability of future conflict.[604] In light of this potential, Hezbollah's daring operation on July 12, 2006 was intended to accomplish three things: deliver on its *wa'd al-sadiq* ("faithful promise") to secure the release of

---

[601] Harik, *Hezbollah*, 48.

[602] Lara Deeb, "Deconstructing a 'Hizbullah Stronghold'," in *The Sixth War: Israel's Invasion of Lebanon*, *The MIT Journal of Middle East Studies* 6 (Summer 2006): 116, http://web.mit.edu/cis/www/mitejmes/; Norton, *Hezbollah*, 132.

[603] These "rules" were generally followed by both sides following the Israeli withdrawal in 2000, and formed a common understanding for engagement. The general outline was that neither side would purposefully attack civilians, that Israel would only be attacked in retaliation for attacks on Lebanon, and that both sides would use proportionality in any attacks. The best analysis of the rules is found in Daniel Sobelman, *New Rules of the Game: Israel and Hizballah after the Withdrawal from Lebanon* (Tel Aviv: Jaffee Center for Strategic Studies, Tel Aviv University, 2004).

[604] Norton, *Hezbollah*, 134–135.

prisoners in Israeli jails, demonstrate Hezbollah's capabilities and will to resist Israel, and show the necessity of retaining these capabilities to Lebanese officials calling for disarmament.[605]

Infiltrating across the border in an area known as milepost 105, near the village of Zarit, Israel, a 20-man Hezbollah team established a complex ambush on the night of July 11.[606] IDF reporting monitors picked up electronic and visual signatures that night, but this information never made its way down to the IDF reserve unit scheduled for a daylight-motorized patrol. At 0900, the patrol was hit with a massive IED and seven anti-tank missiles impacted against the unarmored vehicles. With the vehicles burning, Hezbollah fighters moved forward and extracted two of the wounded soldiers from the wreckage. Simultaneously, other Hezbollah units employed indirect fire, anti-tank missiles, and snipers at other IDF positions in the sector. By the time IDF response units reached the site, nearly an hour later Hezbollah had withdraw, and the few vehicles that crossed over into Lebanon were hit with another complex ambush, resulting in the death of four soldiers.[607]

Israel retaliated with immediate air strikes on 69 bridges in southern Lebanon, designed to frustrate the ambusher's escape, while planning a fuller response. The course of action proposed by Chief of the IDF General Staff Dan Halutz was an air campaign against Hezbollah that would last 48–72 hours. This plan focused on "effects-based operations" that would not strike directly at Hezbollah's military capability, but that would instead exert enough pressure, striking against symbolic Lebanese targets and Hezbollah command infrastructure, that would "force Hezbollah out of southern Lebanon and cause them to disarm."[608] On the night of July 12, IAF jets and artillery began bombardment against targets throughout Lebanon, focusing on Hezbollah's rockets, communications centers, and notable infrastructure. In an interview following the war, Hezbollah's Secretary General, Hassan Nasrallah revealed that the Israeli response and

---

[605] Norton, *Hezbollah*, 135.

[606] Matthews, *We Were Caught Unprepared*, 34.

[607] Ibid., 36.

[608] Ibid., 37.

attacks were unexpected and that the kidnapping operation was not as "clean" as planned.[609] These attacks continued through July 16, with Hezbollah responding with rocket salvos against northern Israel. Halutz was under pressure to do something to stop the rocket attacks and decided to conduct limited battalion-size raids, which was a compromise between solely maintaining air attacks, or launching a full-blown ground offensive to destroy Hezbollah forces.

The first raid commenced on July 17, and the elite *Maglan* unit that penetrated into the Maroun al-Raus area was quickly ambushed, trapped by Hezbollah fighters who were defending a tunnel complex. Reinforcements totaling several battalions, including armored units, the elite *Golani Egoz* unit, and Battalion 101 paratroops, sent in to achieve a breakout, were quickly swarmed by well-armed Hezbollah fighters, who fired anti-tank missiles with devastating effectiveness. As Matt Matthews notes, "Hezbollah's tactical proficiency bewildered the IDF. Hezbollah was not simply hunkering down and defending terrain, but using its small arms, mortars, rockets, and antitank weapons to successfully maneuver against the IDF."[610] With the air campaign proving ineffective against the onslaught of rockets, and the fierce engagements in Maroun al-Raus, Halutz called up the Israeli reserve forces on July 21 to create the impression of a larger force array, as well as ordered forces towards the town of Bint Jbeil, just north of Maroun al-Ras. His intention was to capture the town in a symbolic manner to "create a spectacle of victory" that would lead to a Hezbollah "perception of defeat."[611] With this guidance, only one battalion of the Golani Brigade entered Bint Jbeil from the east, and "at 0530 Companies A and C of the 51st Battalion ran headlong into a withering array of Hezbollah small arms, machine guns, rocket-propelled grenades (RPGs), antitank missiles, mortars, and short-range rockets."[612] The attack at Bint Jbeil utterly failed, and Hezbollah held onto the village through the close of the war. The same disastrous outcome happened throughout the front, and into early August, the Israeli battalion and

---

[609] Hassan Nasrallah, "Interview with New TV," in *Voice of Hezbollah: The Statements of Sayyed Hassan Nasrallah*, ed. Nicholas Noe (Princeton, NJ: Princeton University Press, 2007), 390–391.

[610] Matthews, *We Were Caught Unprepared*, 44.

[611] Ibid., 45.

[612] Ibid., 47.

brigade-sized raids into southern Lebanon had barely penetrated more than a few miles.[613] As reserve units began to move in the border area, it became clear that these forces, comprising nearly 80% of the IDF's ground capability, were seriously undertrained and incapable of fighting such an opponent. Many of the commanders hesitated, due to a growing realization that sending Israeli troops into battle would have been sending them on suicide missions.[614] By August 5, the IDF had nearly 10,000 soldiers in southern Lebanon, but had only managed to penetrate four miles, and the entire border zone remained insecure. In addition, the entire Hezbollah force south of the Litani River consisted of only 3,000 fighters, all original forces from the local areas, with no reserve deployments. On August 11, the United Nations Security Council (UNSC) approved Resolution 1701, which was designed to implement a ceasefire. In response, Olmert and Peretz ordered forces north to the Litani River, as a "kind of show designed to demonstrate to Hizbollah who is the boss," but advancing forces faced fierce resistance and barely managed to advance a mile. A notable action that resulted was Brigade 401's crossing of the Wadi al-Saluki, tanks in column formation, which sprung a complex ambush, resulting in 11 of 24 Merkava tanks hit with anti-tank missiles.[615]

This final attempt at a show of force ended with the August 14 ceasefire, culminating Israeli efforts and allowing them to withdraw multiple units whose fate would have likely been much worse. On the whole, Israeli efforts to accomplish either an effects-based operation to deny Hezbollah southern Lebanon or achieve any substantial military gains failed at strategic, operational and tactical levels. Not only were the Israelis not successful in regaining a buffer zone, but they had little effect against Hezbollah's military capability. Hezbollah rockets struck 160 cities, towns, and settlements throughout Israel, and more than one million people were forced to live in shelters.[616]

---

[613] Daniel Helmer, "Not Quite Counterinsurgency: A Cautionary Tale for U.S. Forces Based on Israel's Operation Change of Direction," *Armor* CXVI, no. 1 (January–February 2007): 8, https://www.knox.army.mil/center/armormag/currentissues/2007/Jf07/1Helmer07c.pdf.

[614] Alastair Crooke and Mark Perry, "How Hezbollah Defeated Israel, Part 2: Winning the Ground War," *Asia Times Online*, October 13, 2006, 5, http://www.atimes.com/atimes/Middle_East/HJ13Ak01.html.

[615] Matthews, *We Were Caught Unprepared*, 54.

[616] David Makovsky and Jefferey White, *Lessons and Implications of the Israel-Hizballah War*, Policy Focus #60 (Washington, DC: Washington Institute for Near East Policy, 2006), 3.

Throughout the conflict, Hezbollah's successful media operations highlighted victory after victory, while showing the horrendous devastation caused by Israeli bombings. The 2006 War demonstrated the increasing importance of information strategy in an age in which media networks are now able to project the battlefield's grim realities—in real time.[617] While Israel attempted to impose its will on Hezbollah through generating significant battlefield effects, Hezbollah demonstrated a sophisticated form of irregular warfare, one not addressed in current doctrinal definitions. In fact, while many analysts debate whether Hezbollah's irregular war fighting is a closer approximation to guerrilla warfare or conventional warfare, it is very likely that it represents something unique; an approach that features a fighting network able to utilize multiple aspects and techniques of war.

1. Israeli Traditional Attack

The July 2006 Israeli invasion was a spur-of-the-moment response, but rested on plans developed to address the growing Hezbollah threat. These plans were developed in the years preceding Hezbollah's kidnapping incursion, and the first was based on a 48–72 hour air campaign against Hezbollah while the second was a ground invasion plan to drive Hezbollah north of the Litani River.[618] Both plans were designed to be activated simultaneously, but Halutz chose to execute a stand-alone air campaign, based on the idea that "…when we hit all these targets Hezbollah will collapse as a military organization."[619] Despite such plans, the Israeli performance in the war reveals a number of strategic issues, looming over their actual war-fighting performance against Hezbollah forces. The primary one is that the IDF believed it could achieve success through a strategic air campaign, without deploying ground forces. Further, when it did finally commit ground forces, it did so haphazardly, without surprise, revealing numerous errors and deficiencies. Overall, Israeli goals in the war were the following.

---

[617] Marvin Kalb and Carol Saivetz, "The Israeli-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict," a paper prepared for the U.S.-Islamic World Forum on February 18, 2007, 2, http://www.brookings.edu/~/media/Files/events/2007/0217islamic%20world/2007islamforum_israel%20hezb%20war.pdf.

[618] Matthews, *We Were Caught Unprepared*, 36.

[619] Shimon Naveh, interview with Matt Matthews, as cited in *We Were Caught Unprepared*, 37.

- Destroy the "Iranian Western Command" before Iran could go nuclear.
- Restore the credibility of Israeli deterrence after the unilateral withdrawals from Lebanon in 2000 and Gaza in 2005, and counter the image that Israel was weak and forced to leave.
- Force Lebanon to become and act as an accountable state, and end the status of Hezbollah as a state within a state.
- Damage or cripple Hezbollah, with the understanding that it could not be destroyed as a military force and would continue to be a major political actor in Lebanon.
- Bring the two soldiers whom the Hezbollah had captured back alive without major trades in prisoners held by Israel—not the thousands demanded by Nasrallah and the Hezbollah.[620]

Organizationally, the IDF was still largely traditional in its structural design, as are most modern militaries and relied on a hierarchical command and control system for orders processing. However, the IDF's combat experience over the years and doctrinal employment stresses a great deal of autonomy on the battlefield. In past wars, lower-level leaders were usually given intent and the resources and latitude required to achieve flexible action in combat. However, during the 2006 invasion, the IDF was subjected to significant organizational friction that resulted in the inability to create autonomy at lower levels. Prime Minister Ehud Olmert and Defense Minister Amir Peretz, headed the organizational hierarchy with control passed to LTG Halutz's General Staff, and the Northern Command under MG Udi Adam. Recognizing the importance of intelligence collection, the Israeli military intelligence organization, AMAN (*Agaf ha Modi'in*) is a separate, independent organization commanded by a general officer as well. The major ground units participating in the invasion were two maneuver divisions, the 91st Division headed by BG Gal Hirsch (composed of eight brigades) and the 162nd Division commanded by BG Guy Tzur (composed of two brigades).[621] Most of the fighting was conducted by the 91st Division, with units from the 162nd brought up and fighting during the last week of the war. Special operations units that participated, mainly conducting

[620] Anthony Cordesman, *Lessons of the 2006 Israeli-Hezbollah War* (Washington, DC: Center for Strategic and International Studies Press, 2007), 6.

[621] William Arkin, *Divining Victory: Airpower in the 2006 Israel-Hezbollah War* (Maxwell AFB, AL: Air University Press, 2007), 163.

deeper strikes into Lebanon and assisting the IAF with targeting, were the *Sayeret Matkal*, *Shayetet 13* naval commandos, and the IAF's *Shaldag* unit. Organizational friction resulted from several factors, but the most often cited was the disconnect between Halutz's focus on air-power effects and ground-force commanders who recognized the requirement for a significant employment of ground forces,[622] which led to conflicting orders as the fighting continued, and further exacerbated strategic errors.

The IDF doctrine entering the second war with Hezbollah was a strange concoction of military theory, incorporating recent theories, such as Effects-Based Operations (EBO) and Systemic Operational Design (SOD).[623] According to Matt Matthews, "the IDF's transient embrace of these post-modern theories at the expense of traditional principles of war is, arguably, one of the strangest episodes in the history of military doctrine."[624] A primary premise of EBO is that attacking an adversary's systems instead of combat formations would produce an effect on the enemy's cognitive domain. General Halutz, a strong proponent of EBO, believes that airpower, supported by precise intelligence, can effectively prevent an enemy from accomplishing actions on the battlefield, without the requirement for ground troops.[625] The primary reason for the attempt at a new doctrine would be to avoid manpower-intensive, and necessarily casualty-producing, conflicts that entail the full commitment of the IDF's resources and

---

[622] Matthews, *We Were Caught Unprepared*, 51.

[623] EBO is a doctrinal theory that seeks to define combat operations through a systems perspective, and is defined as, "operations that are planned, executed, assessed, and adapted based on a holistic understanding of the operational environment in order to influence or change system behavior or capabilities using integrated application of select instruments of power to achieve directed policy aims," as defined in *Operational Implications of Effects-Based Operations (EBO)*, Joint Doctrine Series, no. 7 (Fort Monroe, VA: Joint Warfighting Center, November 17, 2004), 32. SOD is system-based as well, but claims to be "philosophical" in its approach, and was originally formulated by IDF Brigadier Generals Shimon Naveh and Dov Tamari based on a their view of a increasingly complex operating environment. Aspects of SOD are currently incorporated into U.S. Army doctrine under a commander's design process formulated prior to the standard military decision-making process (MDMP). See for example, Milan N. Vego, "Increasing Doctrinal Wisdom," *Joint Force Quarterly*, April 1, 2009 and MAJ Ketti C. Davison, "Systemic Operational Design (SOD): Gaining and Maintaining the Cognitive Initiative," (Fort Leavenworth, KS: United States Army Command and General Staff College, 2006).

[624] Matt Matthews, "Hard Lessons Learned," in *Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD*, ed. LTC Scott C. Farquhar (Fort Leavenworth, KS: Combat Studies Institute Press, 2009), 23.

[625] LTC Abe F. Marrero, "The Tactics of Operation CAST LEAD," in *Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD*, ed. LTC Scott C. Farquhar (Fort Leavenworth, KS: Combat Studies Institute Press, 2009), 84.

by virtue of its reliance on the reserve forces, much of Israeli society as well. SOD sought to apply a war-fighting doctrine that encompasses all the complexities of modern military operations, because the enemy and the environment are a complex adaptive system. However, as Milan Vego states, proponents of SOD "…mistakenly argue that such systems cannot be destroyed but must be pushed into disequilibrium—that is, into chaos."[626] In addition, SOD concepts used overwrought phrases, such as "rendering the enemy incoherent," "consciousness of victory," and "standoff domination of the theater," which only a limited number of individuals understood.[627] Most IDF military officers, used to straightforward and decisive military terminology, simply did not understand much of the new doctrine, and it promoted confusion, even where such concepts might had some relevance. The plan for a large ground force lost out to an EBO-focused air campaign, and when ground operations finally commenced, the confusion brought by the new doctrinal approaches was revealed.

Operationally, the IDF's performance received significant criticism. Numerous reports from the battlefield confirmed a lack of combined arms expertise and proficiency in tactical maneuver, and it was clear that years of COIN operations against Palestinians had greatly eroded the IDF's small-unit combat skills.[628] The overall outcome of the war led to internal soul searching, political in fighting, and a special investigative committee, the Winograd Commission, to investigate the reasons for Israel's performance. In addition to focusing on COIN in the occupied territories, Israeli defense requirements cut large amounts of training and resources from the reserve forces, notable because the reserves comprise 80% of the IDF's total strength. Operationally, the ground forces that advanced into northern Lebanon displayed an overall lack of coordination with air-power assets, and very little of the combined-arms attributes that once generated their success. Overall, the IDF fought in ways that increased Hezbollah's capabilities, as their sporadic

---

[626] Milan N. Vego, "Systems versus Classical Approach to Warfare," *Joint Forces Quarterly* no. 52 (1st Quarter 2009): 42.

[627] Ron Tira, e-mail interview cited in Matthews, "Hard Lessons Learned," 12–13.

[628] Andrew Exum, *Hizballah at War: A Military Assessment*, Policy Focus No. 63 (Washington, DC: The Washington Institute for Near East Policy, 2006), 10, http://www.washingtoninstitute.org/pubPDFs/PolicyFocus63.pdf.

advances provided ample time for Hezbollah to establish ambushes, and the tentative nature of their advances featured little maneuver.[629] Notable operational deficiencies included the lack of training in close urban combat; poor and infrequent employment of special operations forces; a lack of training, preparation, and logistical support for the reserve units; insufficient crew training in armor units, and massive bombings that destroyed infrastructure, but very little of Hezbollah's military capability.[630] The latter proved to be a fundamental flaw in Israel's prosecution of the war, as the destruction they caused, coupled with Hezbollah's anticipatory use of media, generated intense international criticism, which led to the cease fire.

One area in which the IDF displayed notable success was its initial targeting of Hezbollah medium and long-range rockets. IDF sources claim to have destroyed 90% of Hezbollah's medium-range rocket capacity, which may or not be accurate, but it is significant that Hezbollah never fired a single medium or long-range rocket.[631] Tactically, Israel units were caught off guard by the ferocity of Hezbollah's attacks, many of which utilized swarms of 2–3 man cells employing powerful anti-tank missiles against both vehicles and troops. Displaying a lack of combined arms sophistication, on multiple occasions, Israeli commanders spearheaded their advances with armored forces, unaccompanied by the engineers and infantry units, which provide them essential security. Israeli units also a displayed poor understanding of Hezbollah capabilities in relation to the terrain in which they fought. On numerous occasions, IDF troops advanced through constricted terrain and encountered devastating ambushes. Armored forces were engaged in defiles and infantry when clustered in urban areas.

The Israeli invasion displayed little appreciation for wider information strategy, and Israeli strategic decision makers took few efforts to justify the war to the rest of the world, let alone ensure that both tactical and strategic actions were in tune with such a strategy. Surprising, in an era in which it is widely recognized that, "…full-spectrum information activities must be fully integrated with combat operations," senior Israeli

---

[629] Cordesman, *Lessons of the 2006 Israeli-Hezbollah War*, 85.

[630] Ibid., 86–97.

[631] Ibid., 10.

officials and IDF planners launched the 2006 invasion with little integration.[632] This action is not necessarily specific to the 2006 war, however, as Anthony Cordesman states:

> The Israeli government and Israel Defense Forces (IDF) have always tended to see war in terms of their own internal politics and perceptions and to ignore those of other states, cultures, and religions, particularly when dealing with hostile Arab states and movements. The result is that Israel has relied far too much on force and far too little on information operations and politics, and it has repeatedly made strategic mistakes it could have avoided with a more realistic perception of how its enemies and other nations and peoples perceived its action.[633]

In this case, Israel appears to have thought that it could achieve tactical military victories against Hezbollah, while intimidating the Lebanese government with an overall campaign of infrastructure attacks. These flawed assumptions led to significant failures in information strategy, which were aggravated by the fact that what media efforts did exist were largely focused on internal Israeli politics, or in influencing its external supporters.[634] Despite a military doctrine that described a total system of interaction, information was singularly focused on military operations, and neglected the primary opinions it should have sought to influence—global actors and Hezbollah decision makers. Despite having a strategy deliberately focused on intensive bombardment and the destruction of civilian infrastructure and lives, Israel employed too little pro-active measures to mitigate the reaction to such destruction, or its display in the court of world opinion.

2. Hezbollah Network Response

Hezbollah's response to the IDF invasion into Lebanon revealed significant capabilities and displayed a fighting network equipped and capable of inflicting tremendous damage on a first-rate military force. The outcome was largely unexpected,

---

[632] LTC Michael D. Snyder, "Information Strategies Against a Hybrid Threat," in *Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD*, ed. LTC Scott C. Farquhar (Fort Leavenworth, KS: Combat Studies Institute Press, 2009), 104.

[633] Cordesman, *Lessons of the 2006 Israeli-Hezbollah War*, 38–39.

[634] Ibid., 40.

as many within the IDF remembered their dramatic success against another irregular opponent, the PLO, during the last incursion into Lebanon, and failed to account for Hezbollah's transformation during their prior conflict. Hezbollah's initial volley of rockets, numbering in the hundreds, was just the opening salvo in what would be continuous rocket attacks throughout the course of the month. Despite the IDF's best efforts, and extensive bombing by IAF aircraft, Hezbollah managed to employ rocket teams throughout all of southern Lebanon. Even after the IDF commitment of ground forces and the invasion across the Blue Line (page 22), Hezbollah successfully blunted and then stopped multiple Israeli advances into southern Lebanon. Hezbollah's actions on the battlefield were unexpected in multiple ways, including its use of complex defensive structures, excellent concealment, employment of the latest precision weaponry, and remarkable intelligence on Israeli intentions and actions. Its advanced capability differentiates it from classic guerrilla warfare, and in many ways, places it closer to the military capabilities of a nation-state. As Stephen Biddle and Jeffrey Friedman describe, "Hezbollah does demonstrate, unambiguously , that even today's non-state actors are not limited to the irregular, guerrilla model military methods so often assumed in the future warfare debate."[635]

Hezbollah's organization was established based on a social network composed primarily of the radicalized Shi'a community in Lebanon, and has evolved to consist of numerous connections throughout the years. These connections, combined with religious, economic and social aspects, as well as global scale, make it, "…one of the most complex organizations of all Islamist movements in terms of structure and functions…"[636] This organizational complexity defies most analysis, especially those that label the network as either just a "terrorist" organization, or a political party. Hezbollah is deeply embedded in the Shi'a Lebanese society, where its "…social and political activities operate as an integrated and holistic policy network, disseminating the values of resistance while constructing a collective identity derived from the notion of *hala al-islamaiyya*, or the

[635] Stephen Biddle and Jeffrey A. Friedman, *The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy* (Carlisle, PA: U.S. Army War College Strategic Studies Institute, 2008), xvii.

[636] Hamzeh, *In the Path of Hizbullah*, ix.

'Islamic sphere'."[637] These service-oriented networks are fully connected to and an essential part of Hezbollah's notion of resistance, and are not in opposition to the organization's military agenda.[638] Much of Hezbollah's upper-level leadership structure remains unchanged since its founding, but as the grassroots political structure expands, the interconnectedness between the two functions grows as well. Moreover, the Islamic Resistance, which has always been a clandestine network, benefits from a society that is further connected by the same ideals, which makes it easier to recruit, vet, and mobilize willing fighters. As Daniel Byman describes, "many of its recruits were bonded through kinship and regional ties, as well as through a shared ideology."[639] Strictly viewing Hezbollah through organizational terms, it is possible to describe its military arm as a network that works for a hierarchy (formal leadership). In many regards, this military wing resembles an all-channel network, and is broken down into elite fighters, numbering around 1,000, and village fighters, whose numbers are difficult to measure. As Cordesman states:

> During the fighting with Israel, Hezbollah further organized its fighters into small, self-sufficient teams capable of operating independently and without direction from high authority for long periods of time. Although an elaborate system of radio call signs, a closed cellular phone system, and two-way radios allowed these teams to stay in touch with their higher units, a great level of wartime decision-making leeway was given to the junior ranks, largely mitigating the *need* for such communications….As for its counterparts in Chechnya, Iraq, and Afghanistan, Hezbollah's looser structure may have worked to its distinct advantage during the 2006 war, allowing units the flexibility necessary for quick reaction and adjustment to Israeli offensives.[640]

---

[637] Harb and Leenders, "Know Thy Enemy, 192.

[638] Ibid., 193.

[639] Daniel Byman, "Understanding Proto-Insurgencies," *Journal of Strategic Studies* 31, no. 2 (2008): 175, http://dx.doi.org/10.1080/01402390801940310.

[640] Cordesman, *Lessons of the 2006 Israeli-Hezbollah War*, 80–81.

In addition, Hezbollah successfully networked with other organizations and formed ties with unaffiliated villages or other political parties. Notably, a significant portion of the fighters defending Maroun al-Ras were Amal members, and might have produced the first Israeli casualties.[641]

Doctrinally, Hezbollah's response to the 2006 invasion reveals that it no longer fights simply as guerrillas, but displays doctrinal aspects at the cutting edge of irregular warfare. The reason that some label Hezbollah "the best guerrilla force in the world," is largely because it has transformed itself into a fighting network that utilizes modern innovations and technology to fight decisive battles aggressively.[642] Overall, it displayed a defensive doctrine, one highlighted by its remarkably aggressive ambushes and constant barrage of rockets into northern Israel. At the same time, despite being strategically defensive, Hezbollah largely maintained the initiative. As one observer stated, "this was a very good lesson in asymmetric warfare. This was not Israel imposing its battle on Hizballah but Hizballah imposing its battle on Israel."[643] Hezbollah forces utilized the relative simplicity of its weapons and light forces to achieve a level of stealth, which confounded Israeli forces. The largely conventional IDF units had great difficulties in detecting the small or non-existent signature of Hezbollah's light weapons and small maneuver nodes. While part of an overall defense, tunnels connected small groups of fighters, which allowed for local swarming, especially where IDF forces attempted to take key terrain. IDF forces faced small teams that attacked from all directions, and no clear line of separation existed between the advancing IDF in South Lebanon and its Hizbullah foes, with IDF troops repeatedly saying that they were coming under fire from all directions.[644] Simultaneously, Hezbollah's defense displayed sophisticated elements and the highest levels of preparation and planning, reflective of an enemy determined to

---

641 Exum, *Hizballah At War*, 5.

642 Edward Cody and Molly Moore, "'The Best Guerrilla Force in the World:' Analysts Attribute Hizballah's Resilience to Zeal, Secrecy and Iranian Funding," *The Washington Post*, A.1, August 14, 2006, http://search.proquest.com.libproxy.nps.edu/docview/410019829/12F16F8BD2A754B8925/1?accountid=12702.

643 Exum, *Hizballah At War*, 5.

644 Nicholas Blanford, "Hizbullah and the IDF: Accepting New Realities Along the Blue Line," in *The Sixth War: Israel's Invasion of Lebanon, The MIT Journal of Middle East Studies* 6 (Summer 2006): 68, http://web.mit.edu/cis/www/mitejmes/.

fight decisive engagements, not simply "will-o-the-wisp" guerrilla encounters. Further, Hezbollah's use of high-tech weapons, such as the RPG-29 anti-tank missiles and the fielding of the latest in Iranian and Syrian missiles, demonstrates the potential capabilities of irregular forces with nation-state support. The ability to combine these elements produced unique capabilities rarely seen in combination, and reflect a level of doctrinal innovation that took Israeli forces by surprise. In this regard, Hezbollah's doctrine reflects a new level of capability for non-state actors, one gained through its ability to employ synchronize the employment of the most lethal weapons. Rather than rely on its previous guerrilla warfare doctrine, despite its successful application from 1982–2000, Hezbollah adopted a new and unique doctrine, as Nasrallah indicated, "the resistance withstood the attack and fought back. It did not wage a guerrilla war either…it was not a regular army but was not a guerrilla in the traditional sense either. It was something in between. This is the new model."[645]

Operationally, Hezbollah functioned in a very decentralized manner and the flexibility its small units were given enabled them to take the initiative against IDF troops. In addition, its largely local nature provided the ability to be self-sufficient, and eliminated any need for a logistical supply line. Like many irregular fighters, it utilized economy of force to gain advantages in maneuver capability and flexibility. Hezbollah's operational focus centered on the systematic employment of its rocket cells, local attack cells, and elite fighting cells (snipers, bunker defense teams, reconnaissance, etc.). The former provided much of its offensive capability and remained capable of attacks through the duration of the war, and some even sustained attacks through the cease fire, despite being behind IDF lines. The other two elements provided local security for the rocket cells and initiated elaborate ambushes, and moved to key defensive locations as necessary. All these units utilized a complex underground defensive system comprising more than 600 structures. Major Sharon Tosi Moore describes Hezbollah's operations in relation to this underground terrain:

[645] Maryam al-Bassam, "Interview with Hizbollah Leaer Hasan Nasrallah," *Beirut New TV Channel*, aired August 27, 2006, as quoted in Helmer, "Not Quite Counterinsurgency," 8.

> Hezbollah did not fight a static war from these tunnels but rather employed an organized mobile battle plan. Its fighters could hide in, maneuver through, and fight from dozens of prepared battle positions, sophisticated supply bunkers, and complex tunnels dug both inside the villages and into the hillsides. These positions were so well hidden that IDF soldiers did not discover them until they had occupied the area.[646]

This system resulted from a close analysis of how the IDF fought, as one IDF commanders stated, "Hezbollah had spent the years from 2000 to 2006 thinking about the coming war in tactical terms."[647] One of the most notable tactical aspects of the war was Hezbollah's sophisticated use of anti-tank weapons, employed by small teams of three, which displayed considerable ability to engage IDF targets. These weapons were employed in a stand off "swarming" effect against armored columns, being fired in the dozens at times, as well as with great effect against infantry formations and structures. Linking these dispersed elements together was a sophisticated communications architecture, which provided for a significant range of connectivity throughout Hezbollah's forces. Much of this system took Israeli electronic warfare units by surprise as it had advanced protective measures, and was connected by optical fibers to avoid jamming attempts.[648] Further, Hezbollah enjoyed much better intelligence overall, especially at the tactical level, largely because of its familiarity with the local terrain and conditions, but also because it was able to generate a large network of sympathizers.[649] In addition, it took advantage of the overflowing nature of information in Israel's open society, using Internet postings, media reports on Israeli movements, cellular intercepts, and footage of IAF bombing strikes to build a collective picture.

---

[646] MAJ Sharon Tosi Moore, "2006 Lebanon War: An Operational Analysis," in *Joint Center for Operational Analysis Journal* 10, no. 1 (2007): 19.

[647] Exum, *Hizballah At War*, 6.

[648] Cordesman, *Lessons of the 2006 Israeli-Hezbollah War*, 140.

[649] Byman, "Understanding Proto-Insurgencies," 176.

Hezbollah's information strategy is powerful, and derives its strength from a compelling narrative best summarized by the word *Muqwama*, or "resistance."[650] Standing as a model of resistance against Israel, Hezbollah generates vast support, not only in Lebanon, but also throughout the Arab world. This "story" formed a core element of Hezbollah's war-fighting strategy and,

> It was hardly an accident that Hezbollah, in this circumstance, projected a very special narrative for the world beyond its kin—a narrative that depicted a selfless movement touched by God and blessed by a religious fervor and determination to resist the enemy, the infidel, and ultimately achieve a 'divine victory,' no matter the cost in life and treasure.[651]

Buttressed by this powerful idealization of resistance to Israeli aggression, Hezbollah's display of information awareness and its strategy to maximize its benefits stood in stark contrast to Israel's neglect. Hezbollah maximized its ability to control access to the battlefield and the amount of information available, demonstrating that a closed society can control the image and message it wishes to display far more effectively than an open society. In doing so, it was able to portray the Israeli actions as a "disproportionate" response to the July 12 kidnapping, usually by emphasizing the destruction caused by Israeli attacks. To enhance this effect, it limited access to those events and scenes that would benefit this theme and led reporters on tours and even staging or recreating events for media footage. For the most part, journalists followed the Hezbollah-generated script, grateful to get any access as well. These dimensions of information strategy reveal its impact, and it is clear that, "civilians and battles of propaganda and perception are the natural equivalent of armor in asymmetric warfare."[652]

In contrast to the open access showing civilian damage, Hezbollah tightly managed any depiction of a martial image or its military capability, and "throughout the conflict the rarest picture of all was that of a Hezbollah guerrilla. It was as if the war on the Hezbollah side was being fought by ghosts."[653] Hezbollah's skillful employment of

---

[650] Snyder, "Information Strategies Against a Hybrid Threat," 106.

[651] Kalb and Saivetz, "The Israeli-Hezbollah War of 2006," 5.

[652] Cordesman, *Lessons of the 2006 Israeli-Hezbollah War*, 43.

[653] Kalb and Saivetz, "The Israeli-Hezbollah War of 2006," 17.

such tools influenced perception in three important ways: generating an impression of a modern army versus civilians, the "absence" of fighters subtly undercut the claim of using human shields, and it removed Syrian and Iranian military signatures.[654] Further, Hezbollah's concealment of its military image and activities demonstrated a significant use of deception in other ways. Its ability to conceal defensive preparations provides a clear case of tactical deception, with fake bunkers being built to conceal the extensive real ones. This use of "displays" attempts to "…make it [the display] appear other than what it really is," in order to "…make the enemy see what isn't there."[655] It also portrayed an extensive EW intercept capability, bluffing that it could listen in to most Israeli communications, when in reality, it was most likely simply intercepting cell phone and Internet traffic about Israeli forces.[656] The most significant asymmetry in the 2006 conflict had little to do with military weapons, but was the disparity between skillful and effective use of information strategy.

2nd Israel-Hezbollah War				
	Organization	Doctrine	Operations	Information Strategy
Israeli Forces	*Traditional Hierarchy *Little Collaboration	*Effects-Based Air Strikes *Offensive Maneuver *Seize Key Terrain	*Aerial bombardment *Lack of Combined Arms Training	*Focused on Military Effects *No Coherent Approach
Hezbollah Forces	*Formal Leadership Structure *Local networks *Highly connected	*Swarming *Defensive Aim with Aggressive attacks	*Capable Small Unit Tactics *Suicide Operatives *Networked Structure	*Global media access *Pro-active Information Crafting *Strong Narrative

Table 9. Evaluation of the 2nd Israel-Hezbollah War

654 Snyder, "Information Strategies Against a Hybrid Threat," 120.

655 James Dunnigan and Albert Nofi, "Deception Explained, Described, and Revealed," *Victory and Deceit: Dirty Trick in War* (New York: William Morrow, 1995), 19, as referenced in David A. Acosta, "The Makara of Hezbollah: Deception in the 2006 Summer War" (Master's thesis, Monterey, CA: Naval Postgraduate School, 2007), 44.

656 Acosta, "The Makara of Hezbollah: Deception in the 2006 Summer War," 47–49.

3. Analysis of Counter-Network Framework

Despite watching Hezbollah's build up and generation of military capabilities between 2000 and 2006, the IDF misread the threat this irregular opponent posed. Most likely using their experiences against a strictly guerrilla force, the PLO, in 1982, and their COIN operations in Gaza and the West Bank as a basis for decision making, the IDF was caught by surprise in 2006. Their initial aerial strikes were based on significant intelligence, although some were drastically inaccurate, and displayed a few aspects of swarming. However, overall, the IDF demonstrated few of the proposed requirements for effectively countering networks. They sought to counter a highly adapted and socially integrated fighting network with largely conventional means, married to newly formed and debated doctrine. Political indecision and errors in strategic decision making compounded the IDF's efforts, but on the whole, they demonstrated few successes in fighting a sophisticated network.

a. Offensive Swarming

Israeli's initial offense displayed a swarming characteristic, in the form of focused attacks by numerous assets on high value targets, but these aspects were limited to the aerial engagement of Hezbollah's strategic rocket positions and stocks. Beyond the initial aerial engagements of templated Hezbollah positions and infrastructure, the IDF attack against the Hezbollah network failed to swarm systematically against its vulnerable positions. Operationally, especially with regard to its ground offensives, the IDF never gained the element of surprise. Any attempts at generating an operational tempo floundered in the face of strategic indecision. Delays in advancing north provided Hezbollah with additional time to gather intelligence, prepare defenses, and "the IDF also gave Hezbollah ample strategic and tactical warning when it finally did decide to move north."[657] Pulsing relies on the ability to generate intelligence, and but is closely tied to the capability to illuminate the enemy, which must be synchronized with operational efforts. The processes that would facilitate pulsing, both generating intelligence and an

[657] Cordesman, *Lessons of the 2006 Israeli-Hezbollah War*, 84.

ability to swarm against targets, were simply not present in Israel's largely conventional maneuver operations. Likewise, the employment of special operations units for targeting purposes achieved little strategic gains, and such strikes were not generated to produce any significant operational tempo. Israeli press accounts depict only 20 deep operations by Israeli special operations units, the full results of which are still classified.[658] Overall, however, the use of special operations did not affect the war.[659]

b. Illumination

Israel's strategy focused primarily on eliminating Hezbollah as a military threat and IDF actions revealed how little they appreciated Hezbollah's true strength. Beyond the sophisticated technology it received from Syria and Iran, Hezbollah's ability to conceal the entire range and intermeshing of its political, social, and military capabilities provided its most significant advantage in the 2006 War. As Cordesman noted, "the ability to fight on local religious, ideological, and sectarian grounds that the IDF could not match provided extensive cover and the equivalent of both depth and protection."[660]

Israeli intelligence focused primarily on Hezbollah's military positions, templated rocket firing positions, and suspected command and control centers. It employed sophisticated reconnaissance and surveillance assets, as Isaac Ben-Israel, a retired IAF Major General stated, "this was the first large-scale use of UAVs, not only for providing a continuous presence over the entire battle area, but in delivering smart munitions to these very small, well-hidden, moving targets."[661] In addition, Mossad and other Israeli intelligence agencies gathered significant amounts of information on weapons shipments and bunker locations, as well as used agents to "mark" various targets. These efforts featured the infiltration of agents into the Hezbollah network, which

---

[658] Yaakov Katz, "The War in Numbers," *Jerusalem Post*, August 6, 2006, http://www.jpost.com/Israel/Article.aspx?id=30756.

[659] Makovsky and White, *Lessons and Implications of the Israel-Hizballah War*, 55.

[660] Cordesman, *Lessons of the 2006 Israeli-Hezbollah War*, 136.

[661] Barbara Opall-Rome, "Sensor to Shooter in 1 Minute," *Defense News*, October 2, 2006, 1, 6.

demonstrated some capability for illumination efforts. As a result, in the first two weeks, the majority of Hezbollah's longer-range missiles and key command and control locations were destroyed.[662]

However, this focus on significant military capabilities and high-end threats only aided efforts in the initial strikes of the war, and was not matched by efforts to understand Hezbollah's entire network and way of fighting. The level of information the IDF received may have been significant for conducting stand-off strikes, but it was not commensurate with the requirements to illuminate an entire network. For IDF ground offensive success, significantly greater illumination effort was required at the operational and tactical levels. Despite Israel's success in previous counter-terrorism efforts, and its beliefs in the necessity of HUMINT, its "…apparent failure to recruit or retain human sources within Hezbollah explains, therefore, the futile attempts to target the organization's leaders for elimination."[663] These failures are based on Israeli' prioritization of technical development over human collection, but also reveal Hezbollah's efforts at compartmentalization, communications security, and counter-intelligence measures.[664] Efforts focused on understanding the interconnections between fighters and technology, linking operational activity to the social networks generating it, and providing time for focused exploitation to drive operational efforts. While these efforts require extensive preparation and may require changes to the strategic pace of the campaign, Israel efforts that focused primarily on military capabilities missed the significance of the illumination required.

c. Information Disruption

As previously discussed, Israeli information strategy was not attuned to the enemy or the type of war it was fighting. As a result, it displayed some aspects of

---

662 "Israel Intelligence in the Second Lebanon War," *Jane's Intelligence Digest*, September 15, 2006, http://jiwk.janes.com/MicroSites/index.jsp?site=jiwk&pageindex=doc_view&K2DocKey=/content1/janesdata/mags/jiwk/history/jid2006/jid70085.htm.

663 Uri Bar-Joseph, "Israel's Military Intelligence Performance in the Second Lebanon War," in *International Journal of Intelligence and Counterintelligence* 20, no. 4 (2007): 594, http://dx.doi.org/10.1080/08850600701472970.

664 Bar-Joseph, "Israel's Military Intelligence Performance in the Second Lebanon War," 595–596.

information disruption, but neglected others. Rather than negating Hezbollah's narrative, it played right into it, which provided demonstrable and vivid examples of Israeli aggression. Israeli air strikes against urban areas, and in particular, the strikes against the "Hezbollah stronghold" of al-Dahiyya in the southern suburbs of Beirut, produced such outrage that Israel's strategic communications became fixated on defensive justification. Entire villages in the south of Lebanon were flattened, nearly a million civilians were displaced, and estimates of infrastructure damage range from 3–8 billion dollars.[665] By focusing an impressive amount of firepower and devastating aerial attacks against civilian infrastructure, whether "associated" with Hezbollah or not, Israel reinforced Hezbollah's narrative, rather than negated it. Some analysts, such as Reinoud Leenders, make the case that Israel actually shored up a Hezbollah narrative tarnished due to political infighting, competitive Lebanese politics, and relative peace with Israel.[666] Further, tactical successes, such as fighting back Israeli elite units at Bint Jbeil, provided much needed capital to develop the heroic image of Hezbollah military capability.

Israeli efforts to deny, or channel communications, mainly focused on attacking Hezbollah's media capability. Strikes against the five-story headquarters of Al-Manar television in south Beirut occurred during the first night of strikes, even before Israel attacked leadership targets, and were followed up with subsequent attacks, as well as strikes against other media transmission stations.[667] In addition, Israel also conducted extensive jamming and cyberwarfare, and managed to corrupt Al-Manar broadcasts with inserted Israeli messages and programming.[668] However, efforts to silence Al-Manar achieved little as the signal re-appeared within minutes of targeting and Hezbollah was able to continue broadcasting throughout the conflict.

---

[665] Deeb, "Deconstructing a 'Hizballah Stronghold,'" 115.

[666] Reinoud Leenders, "How the Rebel Regained His Cause Hizbullah and The Sixth Arab-Israeli War," in *The Sixth War: Israel's Invasion of Lebanon*, *The MIT Journal of Middle East Studies* 6 (Summer 2006): 38, http://web.mit.edu/cis/www/mitejmes/.

[667] Arkin, *Divining Victory*, 112.

[668] Barbara Opall-Rome, "Israel May Disrupt Commercial Broadcasts," *Defense News*, August 28, 2006, 28, www.oss.net/dynamaster/file_archive/060831.

Multiple reports show that Israel conducted collection operations against Hezbollah's communications and the Lebanese communications infrastructure, but most of this collection was prior to the start of the conflict.[669] Israel's intelligence agency, AMAN, collected extensive information on Iranian and Syrian arms shipments, locations of medium and long-range rockets, and bunkers and tunnel locations. This information guided the initial aerial strikes in the first part of the war, but such collection efforts contributed little to efforts of the IDF troops at the operational and tactical levels. In addition, extensive efforts by the Mossad to identify Hezbollah command and control systems prior to the air campaign were not initially acted upon, and a lack of follow-on operational targeting resulted in no Hezbollah senior leaders being killed.[670] Tactically, the IDF was unaware of the exact location of many of the bunkers and tunnel positions due to their concealment by Hezbollah's extensive deception efforts. Once the ground forays of the war began, little collection efforts to guide advancing units occurred, many of which were caught in complex ambushes as a result. Ground commanders had little or no "real-time" intelligence on Hezbollah forces or positions, despite the extensive collection capacity fielded by the IDF.[671]

Israeli displayed no strategic deception prior to the invasion, and instead slowly telegraphed nearly every move. The initial air campaign caught Hezbollah by surprise, but merely because the scale of the response was unexpected. The halting manner in which ground forces crossed the border gave Hezbollah plenty of warning, but at the least, could have featured different forms and direction of maneuver to deceive the Hezbollah defenders.

d. Fusion

Doctrinally and organizationally, little fusion existed on the Israeli side of the conflict. Most of the Israeli intelligence assets focused on the strategic level, identifying Hezbollah capabilities, but failed to synchronize these efforts with the

669 Bar-Joseph, "Israel's Military Intelligence Performance in the Second Lebanon War," 585, 593.

670 Ibid., 588.

671 Exum, *Hizballah At War*, 4.

information maneuver units required. Even the Interim Report produced by the Winograd Commision concluded, "…in the years that preceded the war, AMAN provided its political and military consumers with a comprehensive, reliable and a correct picture of Hezbollah," but at the same time, also concluded, "at the tactical level the intelligence picture was less clear and exposed significant gaps."[672]

Indecision at the policy and command levels led to a lack of shared intent and purpose during operational execution. While the unique doctrinal frameworks proposed by Halutz and others contributed to confusion during the war, poor decision making led to a clear vision and intent for what Israeli forces hoped to accomplish at the operational level.[673] Initially basing its policy decisions and application of military force on a doctrine that promised swift results with little regard for the fundamentals of ground warfare, Israel never truly developed and diffused a shared purpose throughout the force.

Connectivity between IDF units, especially the combined arms integration that is an Israeli hallmark, was notably absent. This lack of integration between IDF units was exacerbated by an overall lack of collaboration between all elements involved in the war, from the IAF to AMAN and maneuver units on the ground. Nearly 30 years of lower-intensity employment in COIN operations and a lack of training, revealed a serious drop in Israeli capability since its vaunted battlefield victories. Collaborative systems that fused intelligence and operational experience did not exist, and as a result, bureaucratic competition led to insufficient examination of existing intelligence, and a failure to understand what was required in view of the threat. Israeli intelligence gathered significant quantities of information prior to the war, but much of this intelligence was not shared with operational units and its tactical significance was unexploited.[674] The reasons for this were twofold; the first was that much of the information was classified at levels that prevented sharing with tactical units, and the second was a lack of integration between intelligence and operational elements that would have enabled collaboration. At

672 "The Commission for the Investigation of the Battle in Lebanon in 2006, the Second Lebanon War," *The Winograd Commission Report*, an Interim Report, April 30, 2007, 58, http://www.cfr.org/israel/winograd-commission-partial-report/p13228.

673 Matthews, *We Were Caught Unprepared*, 62.

674 "Israel Intelligence in the Second Lebanon War."

the tactical level, "…the interaction between intelligence officers and their consumers in the IDF was ineffective," which contributed such instances as AMAN having intelligence of anti-tank guided missiles (ATGMs), but not discussing this information with operational commanders who could understand its significance and develop counter-tactics.[675] As the Winograd Committee reported, the main problem in combat performance was the lack of a doctrinal system that fused intelligence with operational insights, and "the limit of the intelligence to translate a large part of the information it had…into the operational language used by the fighting forces."[676]

G. CONCLUSION

The long-term outcome of the Israel-Hezbollah conflict may still be uncertain, but it provides numerous definitive lessons, which significant implications for irregular warfare. The primarily guerrilla war Hezbollah fought against the Israeli occupying force between 1982–2000 highlights the potential for a irregular opponent against a much superior traditional military force. Israeli forces discovered the difficulties between successfully invading a country and achieving stability with an occupying force. Throughout much of this conflict, the IDF focused on maintaining control of terrain, ensuring a border zone, but did so using largely static, traditional methods. Hezbollah confronted this strategy with a combination of aggressive guerrilla action, launching significant attacks as IDF and SLA border forts, and an overall outreach that gained the support of and mobilized much of southern Lebanon. A reflection of this aggressive action, and commitment was the innovative use of suicide bombing against IDF targets. These bombings significantly damaged IDF command and control and intelligence collection, but more importantly, demonstrated that the growing strength of Hezbollah's military power. Reinforcing these dramatic terror attacks was an information strategy that portrayed Israel as a heavy-handed occupying force, and highlighted Hezbollah's resistance capability. Israeli bombings and raids grew increasingly ineffective in the face of growing popular disproval for the war in Lebanon, and small changes, such as

675 Bar-Joseph, "Israel's Military Intelligence Performance in the Second Lebanon War," 596.

676 "The Commission for the Investigation of the Battle in Lebanon in 2006, the Second Lebanon War," 58.

attempting a more aggressive targeting effort, came too late. Overall, the conflict reveals basic truths about irregular warfare, highlighting the critical importance of a purposeful policy backed by a robust information strategy, as well as the potential for a disciplined guerrilla force in a war of attrition. It also demonstrates the ability of a network to employ multiple forms of warfare by relying mostly on guerrilla warfare during this conflict, but shows increasing capabilities as the war progressed and they forced the Israeli forces out of Lebanon. In revealing such basic aspects of conflict, it serves a useful comparison, and at the time, a harbinger of the unique aspects of the war to come.

The 2006 War with Hezbollah provides a near laboratory-like test of a traditional military attacking a network-based organization. As many observers have noted, "Hezbollah acted as an informal and adaptive 'distributed network' of small cells and units that were acting with considerable independence and were capable of rapidly adapting to local conditions using media reports, verbal communications, and the like."[677] The conflict was notable not only for the asymmetries in military force on each side, but more significantly, for the tremendous asymmetries of motivation and will between the two combatants. In addition, it highlights the gap between loose political goals and military strategy, and the requirement for an effective grand strategy that unites the two and is reinforced with a meaningful information strategy. Information is truly a powerful weapon, as U.S. military analyst Steve Fondacaro states, "the new element of power that has emerged in the last thirty to forty years and has subsumed the rest is information. A revolution happened without us knowing or paying attention. Perception truly now is reality, and our enemies know it." [678] While some debate occurs about who "won" the war, it is clear that in much of the world, the perception is that Hezbollah won. In addition, it is possible that Hezbollah's true military capability and will to resist was not fully tested. It is likely that Hezbollah reserved the majority of its defense and forces for key actions deeper into Lebanon, and especially, the defense of the Litani River, where it is known that its best anti-tank teams were positioned. The 2006 War revealed a powerful organization, a fighting network whose unique doctrine complimented its

[677] Cordesman, *Lessons of the 2006 Israeli-Hezbollah War*, 134.

[678] Packer, "Knowing The Enemy," 65–66.

organization and provides an example for a new, or "hybrid" form of warfare. Ironically, while many reports focus on Iranian support to Hezbollah, "the fighters of Hizballah have acquired infinitely more combat experience and tactical *nous* than their Iranian sponsors, leading one independent observer to wryly note that Hizballah trains Iran, not the other way around."[679] In light of the IDF's performance against such a fighting network, "the value and capability of such asymmetric net-centric warfare and comparatively slow moving wars of attrition should not be exaggerated."[680]

Israeli Counter-Network Performance				
	Offensive Swarming	Illumination	Information Disruption	Fusion
1st Israeli-Hezbollah War	-	-	-	-
2nd Israeli-Hezbollah War	+	-	-	-

Table 10. Overall Israeli Performance Against Hezbollah Fighting Networks[681]

The IDF performance against such a network reveals significant gaps in its ability to meet the requirements of the proposed counter-network framework. The IDF displays only slight counter-network capabilities, despite historically demonstrating greater capacity in such areas as decentralized combined operations. Overall, the outcome of the 2006 War reveals significant shortfalls, both the IDF's own basic doctrine and training, and in comparison with effective counter-network operations.

The IDF never sought to swarm against Hezbollah, deciding instead to expand its limited air campaign into a very linear, traditional ground offensive. This offensive consisted of brief forays by multiple independent units, and the common assumption appears to be that they were facing a guerrilla threat, such as the PLO, that would be easily overwhelmed by superior force. The brief raids across the border and the slow and

679 Exum, *Hizballah At War: A Military Assessment*, Policy Focus #63, 7.

680 Cordesman, *Lessons of the 2006 Israeli-Hezbollah War*, 136.

681 This basic table highlights the near-complete lack of Israeli performance of the counter-network variables, and the differences in its approach to each conflict.

deliberate advance towards the end of the war were still met with significant resistance. Overall, the sporadic pace of operations produced little resembling an operational tempo that would pressure a fighting network.

Israeli intelligence displayed significant capability for identifying targets and facilitating the initial IAF strikes, but beyond this, there was little that demonstrated illumination. Israel largely ignored the social ties that provided Hezbollah with such a significant advantage, and its near-complete lack of HUMINT capability produced little useable infiltration attempts or use of exploitation. Technical collection, much of which provided the initial targeting templates, lost much of its usefulness as forces on the ground wrestled with the dynamic, and largely concealed, nature of Hezbollah's fighters. An approach that sought to achieve illumination of Hezbollah's capabilities might have sought more of a provocation strategy and forced Hezbollah to reveal more of its forces operationally.

Israel's information strategy failed to comprehend the environment that IDF forces were operating in, and military tasks were not synchronized with a realistic information disruption campaign. Israeli actions failed to negate Hezbollah's purpose, and in fact, significantly reinforced its image as the vanguard of Lebanese and Arab resistance. The openness of Israeli society and the comparative discipline imposed by Hezbollah produced a very lopsided demonstration of information awareness and employment. Further, Israel's military actions served to reinforce each stereotype Hezbollah projected, from wanton aggression against civilians to weak military performance.

Fusion requires a high degree of connectivity between elements, connectivity that is based primarily on doctrinal principles, which promote organizational shaping. The disconnect between policy, military actions, and operational capability reveals a lack of fusion throughout the IDF's performance during both the 1982–2000 occupation and the 2006 War. This lack of fusion appears to be based primarily on the multiple organizations and hierarchical structure of the IDF. Further, although Israel's performance in lower-intensity conflict, such as Gaza and the West Bank, demonstrated a capability for

operational and intelligence integration, these aspects were not incorporated into a doctrine that would produce success in a high-intensity environment against a robust fighting network.

This analysis of Israel's two major conflicts with Hezbollah demonstrates the differences between classic guerrilla warfare and network-style warfare. In the first conflict, Israel's successful invasion and expulsion of the PLO provided a baseline for analysis that revealed the shortcomings of a hierarchical guerrilla organization lacking an integrated local social network, while demonstrating Hezbollah's growing capability. Further, the 2006 War provides a strong example of a traditional modern military denied its goals by a much smaller force. Despite facing a modern fighting network, the Israeli military conducted a deeply flawed campaign demonstrating little of the requirements for effective counter-network warfare. Israel expected to bomb both Hezbollah and the Lebanese government into submission by targeting the former's military capability and the latter's infrastructure. The failure of this policy led to the employment of ground forces, which floundered against a modern fighting network. Israel's performance served notice to the rest of the world, and has since forced dramatic internal changes and revisions in organization, doctrine, operational methods, and most significantly, use of information strategy.

VI. U.S.—AL-QAEDA IN IRAQ CASE STUDY

> If you concentrate exclusively on victory, with no thought for the after effect, you may be too exhausted to profit by the peace, while it is almost certain that the peace will be a bad one, containing the germs of another war.[682]
>
> - Basil H. Liddell Hart

> Sharpen your swords and burn the earth under the feet of the invaders.[683]
>
> - Abu Mus'ab al-Zarqawi

A. CASE STUDY OVERVIEW

The clash between the United States-led coalition that toppled Saddam Hussein and AQI provides a noteworthy case study that highlights modern professional militaries opposed to a complex fighting network. This case study features a primary clash between the most advanced modern military on the globe and a diverse, loosely organized network of insurgents armed almost exclusively with light weapons. This focus on AQI examines its formation and rise to power as the most deadly insurgent group countering the U.S.-led coalition and developing Iraqi forces. AQI rose out of an insurgency following the U.S. invasion in 2003, but like many other fighting networks, it is also a terrorist organization. The devastating violence it inflicted primarily against civilians, inside Iraq and in surrounding countries, marks it as a particularly brutal terrorist organization, despite its initial growth within a popular insurgency. In this regard, the study of AQI provides noteworthy insights into one of the most robust terrorist organizations, and perhaps, the most violently active, in modern irregular warfare.

As in previous case studies, the fight against AQI is examined in two sequential sections, with a final comparison of performance between both. The reason for this delineation is a series of events that produced a different environment and combatant interactions between the two different phases of the war. The initial section focuses on

---

[682] Basil H. Liddell Hart, *Thoughts on War* (London: Farber and Farber, 1944), 129.

[683] Message from Abu Musab al-Zarqawi, April 6, 2004, quoted in Jean-Charles Brisard, *Zarqawi: The New Face of Al-Qaeda* (New York: Others Press, 2005), 96.

the rise of AQI as part of a growing insurgency that reached a violent climax in 2006 with a sectarian civil war. While U.S. forces hunted for the remnants of the Ba'athist hierarchy, what would become AQI began as a growing group of jihadist-inspired fighters who would wreak havoc on coalition efforts to create post-war stability.[684] AQI would go on to terrorize both coalition forces and Iraqi civilians with its increasingly violent tactics before instigating a deeply divisive civil war pitting Sunni versus Shi'a. Along with the civil war, the death of AQI's founder, Abu Mus'ab al-Zarqawi, and the formation of the new Iraqi government ended an increasingly violent phase of the war. The second section of the case study begins with the first part of 2007 and the understanding that few hard lines of demarcation exist in describing events of this scope. A surge of U.S. forces, a change in strategy, and relentless targeting of AQI elements all mark the second phase of the war, which saw a Sunni shift to support coalition efforts and a significant drop in violence. While the war in Iraq against AQI continues, the Iraqi government, supported by U.S. advisers, continues to dismantle the AQI network and for now, it poses no significant threat to Iraqi stability.

B. IRAQ OVERVIEW

The Mesopotamian region of modern day Iraq is called the "cradle of civilization," and the country's history and central position in the Middle East make it a crossroads for trade and a flashpoint of conflict. Sharing borders with Jordan, Syria, Turkey, Iran, Saudi Arabia, and Kuwait, Iraq sits in the center of the region. Geographically, the notable features of Iraq are the Zagros Mountains to the north along the border with Turkey, the al-Jazeerah Desert in the west and south along the border region with Syria, Jordan, and Saudi Arabia, and the Tigris and Euphrates Rivers.

[684] The use of *jihad* and *jihadist* in this case study reflects common, but not altogether accurate, terminology and is maintained for ease of description. In fact, the uses of *jihad*, *jihadist*, and *mujahidin* actually reinforce such enemy combatants' legitimacy in Islamic terms, and serves to buttress their own narrative. Far more effective terms would be those, such as *qital* (murder/war) and *muharibun* (terrorists) as multiple analyses claim. See for example, Shireen K. Burki, "Ceding the Ideological Battlefield to Al-Qaeda: The Absence of an Effective U.S. Information Strategy," in *Comparative Strategy* 28, no. 4 (September 2009): 349–366, http://dx.doi.org/10.1080/01495930903185351.

Figure 15. Iraq and Surrounding Region[685]

Iraq's population, while largely Arab and Muslim, is also composed of the non-Arab Kurdish people in northern Iraq, as well as numerous smaller groups both ethnically and religiously separate. Even within a larger adherence to Islam, deep dissenting opinions separating the Shi'a from the Sunni views, a theological split that strongly

685 University of Texas at Austin, University of Texas Libraries, Perry–Castañeda Library Map Collection, Iraq Maps, http://www.lib.utexas.edu/maps/iraq.html.

influences social and political differences in Iraq.[686] The most commonly accepted numbers for the Iraqi population list 60 percent Shi'a, 15–20 percent Sunni, 18 percent Kurd, and 2–7 percent additional minority groups.[687] Iraq, while having a central government since its foundation, is very much a tribally organized society. Tribes form the social framework for much of Iraqi society, especially in the rural areas, and provide "protection, representation, and a sense of identity," that holds sway even with modern changes.[688] Tribal identity actually has grown stronger in recent times, and 75% of all Iraqis claim identifiable tribal ties, with some of the largest tribes actually having a mix of Sunni and Shi'a. The primary subunit of Iraqi tribes is the *kham*, which includes all those having a single great-great-grandfather, out to five generations. Multiple tribes are unified in a *qabila*, or tribal confederation, which operates at the national and even transnational level in some cases.[689] Tribal organization, and specifically the Sunni Arab tribal structure, played a significant role in the dynamics of the Iraqi insurgency, as "an individual's tribal, clan, or sub-clan membership determines the rights he possesses, the fixed obligations he is expected to meet, and the blood loyalties he must defend."[690]

In the modern era, Iraq's formation resulted from the division of the Ottoman Empire and British colonial rule led to the establishment of an independent monarch in 1932. This monarchy was overthrown in 1958, which led to a series of coups and power struggles that culminated in the Arab Socialist Ba'ath Party taking control in 1968.[691] While originally inclusive, comprising a loose coalition of Kurdish nationalists and Shi'a who viewed themselves as Iraqi Arabs first, the Ba'ath Party that took control in 1968

---

[686] Sandra Mackey, *The Reckoning: Iraq and the Legacy of Saddam Hussein* (New York: W.W. Norton & Company, 2003), 57.

[687] Sharon Ottoman, "Iraq: The Sunnis," *Council of Foreign Relations*, http://www.cfr.org/iraq/iraq-sunnis/p7678.

[688] Lin Todd et al., *Iraq Tribal Study—Al Anbar Governate: The Albu Fahd Tribe, the Albu Mahal Tribe, and the Albu Issa Tribe* (Arlington, VA: Global Resources Group, 2006), 2–2, http://turcopolier.typepad.com/the_athenaeum/files/iraq_tribal_study_070907.pdf.

[689] Glenn Robinson, "Identity Politics and the War in Iraq," in *The Three Circles of War: Understanding the Dynamics of Conflict in Iraq*, ed. Heather S. Gregg, Hy S. Rothstein, and John Arquilla, (Washington, DC: Potomac Books, 2010), 13.

[690] Shultz and Dew, *Insurgents, Terrorists, and Militias: The Warriors of Contemporary Combat*," 203.

[691] Mackey, *The Reckoning*, 196.

was primarily Sunni, experienced and more ruthless in its hold on power.[692] Saddam Hussein fought his way through the Ba'ath Party ranks to assume control of its security force in the early 1960s and he led a tightly controlled group called the *Jihaz Haneen*, or "instrument of yearning" that tolerated no challengers to its control.[693] While multiple Middle Eastern governments were being toppled from within, the Ba'ath Party security forces repressed all opposition and imposed a reign of fear that would allow increased control. Taking the role of the party's strongman, Hussein increasingly gained power until he was the de facto ruler and barely tolerated the formal president Ahmed Hassan al-Bakr, who had built the ruling political circle from their shared al-Tikriti clan. Following bloody internal purges in 1979, Hussein accepted Bakr's resignation and stood as the supreme ruler of the country. Along with gaining political control, the Tikriti Ba'athists imposed a Sunni-dominated cultural perspective on the country, combining elements of Ba'ath doctrine with an emphasis on Iraq's unique history and civilization.[694] This combination served to reinforce the idea of a dominant leader, while covering over sectarian divisions with a strong sense of historical greatness derived from the ancient empires, which ruled Mesopotamia in the past. Implicit in these efforts was the understanding that the Sunni minority held sway over society through its dominance of the key apparatus in the country, the political system, security organizations, armed services, and key ministries controlling finance, education, and essential services. In addition, Hussein and the Ba'ath Party co-opted the tribal power structures, legitimizing the idea of tribes and using sheikhs as a tool to be manipulated, while legitimizing kinship as a principle for selection.[695]

After consolidating power, one of the first challenges facing Hussein was attacks from the growing ranks of Shi'a militants, including the *al-Dawah* Party and other semi-clandestine organizations whose raids and terror attacks threatened the party and led to

---

[692] Phebe Marr, *The Modern History of Iraq* (Boulder, CO: Westview Press, 1985), 205–206.

[693] This group would become the Iraqi security services, or *Mukhabarat*, and would control nearly every aspect of Iraqi society with its regime of terror, Mackey, *The Reckoning*, 201.

[694] Eric Davis, *Memories of State: Politics, History, and Collective Identity in Modern Iraq* (Berkley, CA: University of California Press, 1978), 62.

[695] Amatzia Baram, "Neo-Tribalism in Iraq: Saddam Hussein's Tribal Policies 1991–96," *International Journal of Middle East Studies* 29, no. 1 (1997): 1, http://www.jstor.org/stable/163849.

violent clashes.[696] This internal threat, fueled by a revolutionary Iran, and a desire for increased control in the region, led Hussein to attack Iran aggressively in September 1980, which led to an eight-year war that ranks as the longest conventional war of the 20th century. The war engulfed the two nations, at least a million people died and over 2 million were wounded, at an estimated cost of $1.2 trillion dollars and incalculable social impacts.[697] It ended in a stalemate and ceasefire but decimated Iraq's social fabric, created enormous physical destruction and imposed economic strain that would lead to the next war—sparked by Iraq's invasion of Kuwait in August 1990. The response by an international coalition of forces was the 1991 Gulf War, led by a month-long aerial bombing campaign, followed with an allied coalition that swept into Iraq and liberated Kuwait. The terms of the Gulf War ceasefire at Safwan allowed Hussein to keep his elite Republican Guards and continue flying helicopters, thereby, maintaining his ability to repress Shi'a and Kurdish internal uprisings brutally.

In the decade that followed Hussein's survival in the face of the allied coalition and internal uprisings, Iraq suffered under United Nations Security Council sanctions meant to dissuade Hussein from building his weapons arsenal. Inspectors from the UN Special Commission on Iraq (UNSCOM) would spend much of the decade in a hide-and-seek game focused on the weapons capability of the Iraqi regime, while U.S. aircraft enforced a no-fly zone and struck selected targets to reduce Hussein's capacity.[698] Despite multiple attempts at pressuring Hussein, little succeeded, and even coalition-imposed sanctions began to wear thin in the court of international opinion. Following September 11, 2001, the preventive "Bush Doctrine" led to a full-court press to include Iraq in its list of targets and build a coalition willing to overthrow Hussein and his regime. All of this history built into shaping the events that would follow the U.S.-led coalition invasion of Iraq in 2003.

---

[696] Mackey, *The Reckoning*, 247–249.

[697] Ibid., 235.

[698] John Keegan, *The Iraq War* (New York: Alfred A. Knopf, 2004), 86–87.

C. AQI BACKGROUND

While most of the insurgent organizations in Iraq began after the fall of the Iraqi regime in 2003, al-Qaeda in Iraq had early beginnings. The organization evolved from a salafist jihadi group, *al-Tawhid wal-Jihad* (One Unique God and Jihad), founded by Abu Mus'ab al-Zarqawi, a Jordanian born charismatic leader.[699] As his name depicts, Zarqawi grew up in Zarqa, Jordan and dropped out of school to attend the war in Afghanistan as a young jihadi in 1989. While he missed the war against the Soviets, he participated as a makeshift reporter and then fighter during the battles between Islamist factions and the procommunists, and the civil war that followed. It was there that he met and was influenced by notable jihadist fighters and ideologists, such as Abu Mohammad al-Maqdisi, and attended military training camps run by many of al-Qaeda's early leaders.[700] Returning to Jordan in 1993, Zarqawi was a marked Afghan veteran and formed a cell, *Bayt al-Imam,* with Maqdisi and other Jordanian jihadists. This cell conducted attacks against Jordanian authorities until it was disbanded and Zarqawi and Maqdisi arrested and placed in At Suwaqah prison in 1994.[701] Upon his release from prison in 1999, Zarqawi returned to Pakistan and Afghanistan, and rallied a contingent of Jordanian Islamists who were introduced to and swore allegiance to al-Qaeda by the noted Jordanian confident of Osama bin Laden, Abu Zubaydah.[702] Although welcomed as one of many foreign groups by al-Qaeda, in time, Zarqawi moved his group to the western city of Herat, where he displayed an increasing autonomy, set up a camp disguised as a religious school, and flew a banner at the entrance, which read *Tawhid wal-Jihad*. While in Herat, Zarqawi grew his organization, launched attacks, and established a small community of jihadists in Iraqi Kurdistan as a new front in the jihadist

699 Lee Hudson Teslick, "Profile: Abu Musab al-Zarqawi," *Council on Foreign Relations*, http://cfr.org/publication/9866/.

700 Brisard, *Zarqawi*, 16–26.

701 Loretta Napoleoni, *Insurgent Iraq: Al-Zarqawi and the New Generation* (New York: Seven Stories Press, 2005), 66–72.

702 Brisard, *Zarqawi*, 67.

struggle.[703] Meshing with the Kurdish Islamist group *Ansar al-Islam* (AI) paid dividends through a symbiotic relationship, based on Kurdish funding and contacts in Europe and training and links to al-Qaeda through Iran. These ties became more obvious when Mullah Krekar, the head of AI, was indicted in the wake of the "millennium plot" to bomb tourist targets in Jordan.[704]

When the hunt for al-Qaeda began in 2001, Zarqawi and his group fled Afghanistan and moved across Iran to settle in the mountainous Kurdistan region of Iraq.[705] The network of relationships Tawhid had formed allowed them to establish themselves rapidly in the Sargat region. Zarqawi used this base of operations to move throughout the region to conduct attacks, such as the one that killed the USAID diplomat Thomas Foley in Jordan in October 2002. While Zarqawi and Tawhid used the Kurdistan region as a base, their network ranged from Iran to Syria, and included contacts in Europe. While U.S. Secretary of State Colin Powell cited Zarqawi's presence in Iraq as proof of the country's collusion with al-Qaeda, Zarqawi crossed multiple borders over nine years, facilitated by a network that spanned multiple countries.[706] His long-standing nickname, al-Gharib, or the Stranger, seemed to reflect this level of transient activity, and would be emblematic of his organization's foreign jihadi composition in the years to come.[707]

---

[703] It is likely that this outpost in Kurdistan was formed to provide al-Qaeda leadership with another basing option following the anticipated response to the 9/11 attacks, and at the least continue to provide a conduit for attacks against targets in Jordan and Israel. See, for example, Bruce Riedel, *The Search for Al-Qaeda: It's Leadership, Ideology, and Future* (Washington, DC: Brookings Institution Press, 2008), 96–99; Brisard, *Zarqawi*, 77–80.

[704] Brisard, *Zarqawi*, 82.

[705] Nu'man ibn 'Uthman, former Afghan jihadi, interview in *Al-Hayat*, as cited in, "Former Jihad Fighter in Afghanistan: Al-Zarqawi's Group Adopted the Worst Practices of the Algerian GIA: Their Brutal Actions will Lead to their Isolation," http://www.memri.org/report/en/0/0/0/0/0/0/1256.html.

[706] According to Colin Powell, Zarqawi was the direct link between Iraq and al-Qaeda, but it is likely that most of Zarqawi's enterprise was fairly autonomous and designed to facilitate jihad throughout the region, and it is clear that he spent much of his time in Syria coordinating operations. See for example, Jonathan Schanzer and Dennis Ross, *Al-Qaeda's Armies: Middle East Affiliate Groups & the Next Generation of Terror* (Washington, DC: Washington Institute for Near East Policy, 2005), 136; Loretta Napoleoni, *Insurgent Iraq: Al Zarqawi and the New Generation*, 106. For the full text of Colin Powell's speech see "Full Text of Colin Powell's Speech: U.S. Secretary of State's Address to the United Nations Security Council," *The Guardian*, http://www.guardian.co.uk/world/2003/feb/05/iraq.usa.

[707] Brian Fishman, "After Zarqawi: The Dilemmas and Future of Al-Qaeda in Iraq," *The Washington Quarterly* 29, no. 4 (2006): 22, http://dx.doi.org/10.1162/wash.2006.29.4.19.

The U.S. invasion in 2003 brought a direct assault by U.S. Army SF and Kurdish *Peshmerga* forces against Zarqawi and the AI base in Sarqat, killing hundreds and scattering those that survived.[708] As the larger Iraqi insurgency grew, Tawhid focused on rebuilding itself following the strikes in the north, but its first major attack, in August 2003, which brought international attention, was a suicide attack on the UN headquarters in Baghdad. This noteworthy attack killed the chief of the UN Assistance Mission to Iraq Sérgio Vieira de Mello and another attack shortly after led to the withdrawal of most of the UN staff. Ten days later, a second major suicide attack, a car laden with explosives, killed the Shi'a Ayatollah Mohammed Baqir al-Kaim and hundreds of Shi'a in the Imam Ali Mosque in Najaf.[709] Further major suicide attacks followed against Shi'a worshippers in Baghdad and Karbala on March 2, while they were celebrating the Shi'a holiday of Ashura. Yet, even with these major terrorist bombings, the act that brought the most notoriety was the kidnapping and beheading of U.S. contractor Nicholas Berg in April 2004, by Zarqawi under a *Tawhid wal-Jihad* banner.[710] The savagery of this act shocked watchers, revealing its effectiveness as an act of terror, and with it, Zarqawi sent a message for the world to take notice, as well as a call to other jihadist groups to unite under his leadership to, "…make jihad and brandish the sword that the prophet has sent us."[711] In a letter captured by U.S. forces in January 2004, Zarqawi outlined Tawhid's goals and methods and proposed a formal affiliation with Osama bin Laden's al-Qaeda:

> If you agree with us on it, if you adopt it as a program and road, and if you are convinced of the idea of fighting the sects of apostasy, we will be your readied soldiers, working under your banner, complying with your orders, and indeed swearing fealty to you publicly and in the news media, vexing the infidels and gladdening those who preach the oneness of God.[712]

---

[708] This assault, code-named Operation Viking Hammer, was led by the 3rd Battalion, 10th Special Forces group that advised *Peshmerga* forces and synchronized close-air support during the assault. For more details on this unique strike against a terrorist training camp see Linda Robinson, *Masters of Chaos: The Secret History of the Special Forces* (New York: Public Affairs, 2004), 296–323.

[709] Nimrod Raphaeli, "The Sheikh of the Slaughters: Abu Musa'b Al-Zarqawi and the Al-Qaeda Connection," *Middle East Research Institute*, 4, http://www.memri.org/report/en/0/0/0/0/0/0/1406.htm.

[710] Raphaeli, "The Sheikh of the Slaughters," 5.

[711] Abu Mus'ab al-Zarqawi, May 11, 2004, Videotaped Broadcast, cited in Brisard, *Zarqawi*, 131.

[712] Abu Mus'ab al-Zarqawi, Signed Zarqawi Letter Seized in 2004, in Brisard, *Zarqawi*, 251.

This letter was part of a dialogue between Zarqawi and al-Qaeda senior leadership over his strategy to conduct terror attacks against Shi'a civilians, in an attempt to force division, a matter that became contentious and was always a source of frustration between the leadership elements.[713] However, by late 2004, Zarqawi had sworn *bayat* to bin Laden, and in a response from bin Laden, he was introduced as the "commander of the al-Qaeda organization in the land of the Tigris and the Euphrates," an organization named *Tanzim al-Qaeda al-Jihadi fi Bilad al-Rafidayn* (Al Qaeda Organization in the Land of the Two Rivers, referred to as TQJBR or QJBR).[714] This organization would subsequently be referred to by its shortened form of al-Qaeda in Iraq (AQI) by both group members and the greater Iraqi population, and it assumed a semi-affiliated franchise status of the greater al-Qaeda organization.

D. THE IRAQ INSURGENCY: 2003–2006

The U.S. invasion of Iraq was a showdown between two nation-states, resulting in a rapid victory, but it precipitated a much longer, and in many ways, more complex struggle. The initial invasion of Iraq in March 2003 featured unprecedented joint operations and a rapid advance to penetrate deep into Iraq from the north, west, and south, which resulted in the rapid disintegration of Iraqi forces, and their almost "mysterious" evaporation from the battlefield. U.S. and coalition special operations forces played a large role in the success of the initial invasion, which was a "lightning campaign" that lasted only 21 days.[715] The Iraqi military was truly "overmatched" on the battlefield by the coalition's combination of forces and capabilities, which featured, "…integrating ground maneuver, special operations, precision lethal fires, and non-lethal

[713] Napoleoni, *Insurgent Iraq*, 159–167.

[714] Osama bin Laden, as quoted in "Osama Bin Laden to the Iraqi People," MEMRI Special Dispatch no. 837, *Middle East Research Institute*, 3, http://www.memri.org/report/en/0/0/0/0/0/0/1286.htm; Peter Bergen, "After the War in Iraq: What Will the Foreign Fighters Do?" in *Bombers, Bank Accounts, and Bleedout*, ed. Brian Fishman (West Point, NY: Combating Terrorism Center, 2007), 109.

[715] Keegan, *The Iraq War*, 1.

effects."[716] Yet the rapid success of the invading forces in this first phase of the war quickly gave way to a far more difficult occupation. Former Iraqi dissident Ali Allawi explained, "the euphoria that accompanied this effortless victory quickly gave way to increasing bewilderment as to what to do with the 'prize,' as the occupiers came face to face with the realities of post-Saddam Hussein Iraq and the mysteries of this most complex of countries….Nothing…could have prepared the Coalition…for what they actually found."[717]

By mid-July 2003, General John Abizaid, the new U.S. Central Command Commander, described the "postwar" levels of violence as a "classical guerrilla campaign," and that "…the mid-level Ba'athist threat is the primary threat that we've got to deal with right now."[718] Yet even at that point, clandestine Ba'athist organizations were being overwhelmed and subsumed into a growing network of diverse and loosely affiliated insurgent groups. The majority of these groups were composed of Sunni Iraqi's whose resistance to the U.S.-led occupation took strongest root in the Sunni tribal areas along the Euphrates and Tigris River valleys, and in such cities as Fallujah, Ramadi, Samarra, and Mosul. While most Shi'a, having been oppressed under Saddam Hussein's Sunni-dominated rule, initially welcomed the overthrow of the regime, Iraq's Sunnis lost much of their pre-eminent status.

The combination of Sunni disenfranchisement exacerbated by Ambassador Paul Bremer's decision to purge the government of Ba'athists and then disband the Iraqi Army produced a volatile mix of opposition. The insurgency that grew after the 2003 occupation of Iraq was different from the unified and systematic efforts featured in Mao's "people's war," but instead consisted of a diverse collection of multiple groups with

---

[716] Anthony Cordesman uses the term "overmatching power," to reflect the idea that "overwhelming force" may not be the best measure of combat power in the 21st century, and cites General Tommy Frank's discussion of integration during a brief before the U.S. Senate Armed Forces Committee on July 9, 2003 in Anthony Cordesman, *The Iraq War: Strategy, Tactics, and Military Lessons* (Westport, CT: Praeger Publishers, 2003), 3.

[717] Ali A. Allawi, *The Occupation of Iraq: Winning the War, Losing the Peace* (New Haven, CT: Yale University Press, 2007), 1.

[718] General John Abizaid, Department of Defense briefing transcript, July 16, 2003, cited in Anthony Cordesman, *The Iraq War: Strategy, Tactics, and Military Lessons* (Westport, CT: Praeger Publishers, 2003), 518.

different aims. This complex, dynamic environment pitted over 40 named insurgent groups, each with their own ideological variations, motivations, and even tactics against a coalition of countries seeking to establish a central Iraqi government. Hardly a classic guerrilla war, as Bruce Hoffman stated, "…what is found in Iraq is the closest manifestation yet of netwar, the concept of warfare involving flatter, more linear networks rather than the pyramidal hierarchies and command and control systems (no matter how primitive) that have governed traditional insurgent organizations."[719] The majority of these groups were nationalistic in orientation, either fighting against the coalition occupation and/or to preserve their cultural, political and economic status. In addition, Iraq became a destination for transnational jihadis, attracted to the latest jihad to follow Afghanistan, Somalia, Bosnia, Chechnya, and other flashpoints. Zarqawi's QJBR, and then AQI, became a national organization to gravitate to, with its external networks, multi-national composition, and global salafist orientation. As Andrew Phillips stated, "in the chaotic aftermath of Saddam's fall Iraq became an ideal venue for deterritorialized [sic] nomadic jihadists to prosecute their dream of unifying the *ummah* under the banner of a universal caliphate."[720] Despite the capture of Saddam Hussein and the elimination of the Ba'ath Party hierarchy, the insurgency grew in size and scope.

By April 2004, the insurgency flared into major combat when Sunni insurgents established a base of operations out of the city of Fallujah, and backed a growing foreign jihadist presence. The savage killing and celebration of the deaths of four contractors in the city sparked a U.S. Marine-led invasion against the growing jihadist presence. Led by AQI, a significant number of Sunni jihadists fiercely resisted U.S. Marine efforts to retake the city. After the Marines withdrew, the city became a further hotbed of insurgent activity, with AQI and other jihadist groups imposing harsh, puritanical practices based on sharia. These efforts, such as imposing salafist ideology, soon led to more coercive measures and horrific acts of violent intimidation as AQI sought to impose acceptance on the population by force. Also in the same month, the revelation of prisoner abuse at Abu

[719] Bruce Hoffman, "Insurgency and Counterinsurgency in Iraq," *Studies in Conflict and Terrorism* 29, no. 11 (2006): 115, http://dx.doi.org/10.1080/10576100500522173.

[720] Andrew Phillips, "How al-Qaeda Lost Iraq," *Australian Journal of International Affairs* 63, no. 1 (2009): 70.

Ghraib prison greatly damaged the U.S. coalition's credibility and added fuel to the already blazing insurgency. In November 2004, U.S. forces retook Fallujah in a massive urban battle, Operation Al Fajr ("New Dawn" in Arabic), but much of the AQI leadership and senior operatives had fled the city well in advance and sought to regain control in other areas through the Euphrates River Valley (ERV).[721]

The election of the Iraqi Transitional government dominated the early part of 2005, but its boycott by Sunni tribes showed that the main core of the insurgency still refused coalition and Iraqi government control. In addition, the large numbers of Kurdish and Shia participation ensured that the government was largely dominated by Shi'a parties, which furthered the threatened perception of the Sunnis. Fighters that had fled Fallujah were being pursued in the ERV and the northern Ninewah Province to which they had fled, and some even attempted to impose the same levels of control in Tal Afar. The newly elected Iraqi government became solidly Shi'a controlled, and more power was passed to newly formed elements of the Iraqi Army. In an effort to put Iraqis "in-the-lead," U.S. forces in and around Baghdad were pulled back to their forward operating bases (FOBs), believing that this would also reduce the escalating violence.

The al-Askari, or "Golden," Mosque bombing in Samarra on February 22, 2006 resulted in no injuries, but the explosion destroyed much of the mosque, one of the holy sites of Shi'a Islam, and sparked intense sectarian violence. AQI claimed the attack, justified by Zarqawi's strategy that, "our fighting against the Shi'a is the way to drag the nation [of Islam] into the battle," and after countless high-profile bombings against Shi'a targets, the al-Askari mosque bombing provided the final straw.[722] The bloodletting that followed split sectarian fault lines, and resulted in a sectarian civil war that raged for well over a year, which resulted in the ethnic cleansing of whole sections of Baghdad, and the weak, Shi'a-dominated government "…becoming an open partisan in a nasty civil war between Sunni and Shiite Arabs."[723] While Zarqawi was killed in a U.S. airstrike at a

---

[721] John R. Ballard, *Fighting for Fallujah: A New Dawn for Iraq* (Westport, CT: Praeger Security International, 2006), 54; Hashim, *Insurgency & Counter-insurgency in Iraq*, 45.

[722] al-Zarqawi, *Signed Zarqawi Letter seized in 2004*, 247.

[723] James D. Fearon, "Iraq's Civil War," *Foreign Affairs* 86, no. 2 (March–April, 2007): 3, http://www.jstor.org/stable/20032280.

house outside of Baqubah in June 2006, the clash he unleashed pitted Sunni versus Shi'a and would be the dominant feature throughout 2006, and threatened the very idea of Iraq itself.[724]

1. U.S. Invasion and Occupation

The initial invasion of Iraq, Operation Iraqi Freedom (OIF), achieved historical levels of joint synchronized operations, and despite resistance from irregular Iraqi units, swiftly moved towards securing key objectives. The overall invasion forces were relatively small, which demonstrated that force ratios matter less than other elements of combat power and capabilities that were overwhelmingly in the United States' favor. In addition, the invasion made extensive use of U.S. and coalition SOF, combining them in ways that provided additional capabilities. Their employment included subversion, strategic reconnaissance, deceptive maneuver, and, in conjunction with Kurdish *Peshmerga* forces, the truly unconventional direct confrontation and defeat of the Northern Iraqi Army. This initial success highlighted integration in support of coalition forces, and overwhelmingly surmounted the "difficulties" associated with the employment of special operations in the support of conventional forces.[725]

However, the initial occupation of Iraq grew problematic almost as soon as the initial objectives were seized. To begin with, U.S. senior leaders failed to understand the complex dynamics of Iraq, had no overall strategy for peacekeeping and stability efforts, and made costly mistakes that fueled growing resentment from Iraq's population.[726] It was, as Kilcullen stated, "a disaster of our own making."[727] In addition, the lack of a coherent focus on the changing situation meant that the war shifted to "…a forward operating base defense plan and a main supply route (MSR) sustainment operation, with

[724] Civilian casualties peaked between September 2006 and January 2007, with 2,700 and 3,800 civilians killed per month, every month. In December 2006 alone, the killings peaked at around 125 per night, more than half within Baghdad city limits. Kilcullen, *The Accidental Guerrilla*, 126.

[725] Kiras, *Special Operations and Strategy*, 14.

[726] Hoffman, "Insurgency and Counterinsurgency in Iraq," 104.

[727] Kilcullen, *The Accidental Guerrilla*, 118.

the force becoming languid and complacent, fixed in an effort just to maintain."[728] U.S. forces, focused on their recent, largely conventional victory, failed to understand that the nature of the environment had changed. "Instead of switching to an unconventional approach for defeating the insurgency, however, the coalition maintained a conventional style in most of its engagements, all the while building bureaucratic systems to emulate garrison activities found on installations in the U.S. and other military compounds throughout the world."[729] Conventional forces that had prepared to fight a war of maneuver, complete with tanks and artillery, were now searching for ways to cope with a new form of opponent, and an asymmetry in warfare that was both difficult to accept and comprehend.[730]

Small teams of U.S. Army SF and other SOF elements understood the changing situation, having prepared and trained for just such an environment, and continued to attempt to influence local security and pursue those responsible for the growing levels of violence.[731] In addition, far-sighted local conventional commanders, usually at the battalion levels, understood the changing dynamics, and instituted policies and local outreach that achieved levels of effectiveness with little to no guidance from higher headquarters. SOF were successfully employed throughout the evolving conflict against numerous insurgent groups, and while the invasion witnessed the largest use of special operations in history, it was actually their performance after the initial phase of the war that would prove the most significant.[732]

The U.S. occupation force was organized as a traditional military hierarchy, one that retained much of the combat headquarters from the conventional invasion. However, despite a change in mission, these larger headquarters remained, providing additional,

---

[728] COL Dominic J. Caraccilo and LTC Andrea L. Thompson, *Achieving Victory in Iraq: Countering an Insurgency* (Mechanicsburg, PA: Stackpole Books, 2008), 3.

[729] Caraccilo and LTC Thompson, *Achieving Victory in Iraq*, 4.

[730] Yossef Bodansky, *The Secret History of the Iraq War* (New York: Harper and Collins, 2004), 396.

[731] COL Chet Richards (Ret.), LTC Greg Wilcox (Ret.), and COL G.I. Wilson (Ret.), "America in Peril: Fourth Generation Warfare in the Twenty-First Century," in *Global Insurgency and the Future of Armed Conflict*, ed. Terry Terriff, Aaron Karp, and Regina Karp (New York: Routledge, 2008), 122, 127.

[732] Finlan, *Special Forces, Strategy and the War on Terror: Warfare by Other Means*, 141.

and at times, competing layer of bureaucracy. Three major headquarters, the Multi-National Forces-Iraq (MNF-I), the Multi-National Corps-Iraq (MNC-I), and the Multi-National Security Transition Command-Iraq (MNSTC-I), provide four and three star level headquarters inside Iraq. These major headquarters provided for division of labor, but also contributed to confusion in strategy and competition for resources, as Colonel Dominic Caracillo recounted, "more specifically, there are too many headquarters in Iraq vying for power and the limited resources available. A running joke in the theater among subordinate commanders, when posed with the challenges of answer to multiple headquarters, was 'never have so few been commanded by so many.'"[733] An excess bureaucracy, combined with many leaders without combat experience at lower levels led to increasing oversight and micromanagement. Caracillo described the effects well, noting, "bureaucracies lead to commands starved for information, which leads to mistrust of subordinate commanders and staff, which in turn leads to countless investigations and overly structured hierarchical command."[734] Further, divisions in higher-level headquarters translated to ambiguous command relations further down the chain of command, which resulted in difficulties in the development of overall capability among Iraqi Security Forces (ISF). Tellingly, the notable successes that occurred from 2003–2006 resulted from tactical units, usually at the brigade-level and below, taking initiative based on the local situation.[735] Notable examples include the 3rd Armored Calvary Regiment (ACR) under Colonel H.R. McMaster successfully providing population-centric security in Tal Afar, the combined efforts of the 2nd Battalion, 503rd Infantry (Airborne) and Army SF establishing a viable police force and security presence in the city of Kirkuk, and the bold clear-hold-build strategy employed by Colonel Sean MacFarland's 1st Brigade, 1st Armor Division (1/1 AD) in Ramadi.

A lack of overall counter-insurgency strategy in the early years of the war reflected a lack of understanding and willingness to accept the situation in Iraq, as well as a lack of coherent doctrine. While some tactical-level commanders understood the nature

---

[733] Caraccilo and Thompson, *Achieving Victory in Iraq*, 12.

[734] Ibid., 25.

[735] Hoffman, "Insurgency and Counterinsurgency in Iraq," 109.

of the environment, and relied on fragments of counter-insurgency doctrine in older manuals, most defaulted to conducting largely military-focused operations, such as direct targeting and large-scale cordon and searches. Many other junior leaders, seeking the most current lessons-learned, built a network of understanding on the website, CompanyCommand.com.[736] The most current doctrinal manual available was the U.S. Army Field Manual 3-7, *Stability and Support Operations*, which was released just prior to the start of OIF. While far too broad to cover COIN details, it did provide useful general guidelines , but it was limited by its assumption that U.S. forces would provide advice and support rather than conduct operations themselves.[737] Realizing that it needed a comprehensive doctrine specific to COIN, the Army released Field Manual Interim (FMI) 3-07.22, *Counterinsurgency Operations*, which elaborated on previous concepts and doctrine. Yet, even this step in the right doctrinal direction was not enough to change practices on the ground, as Austin Long describes in the RAND assessment of U.S. COIN practices from 2003–2006:

> The U.S. military's actual conduct of COIN in Iraq from 2003 to 2005 can charitably be described as highly variable. The military used an array of approaches ranging from firepower intensive raids to population security. This variation seems to have depended partly on understandable differences, such as the region and time period, but mostly appears to be due to different commanders.[738]

Although the establishment of a "COIN Academy" for all incoming leaders commanding in Iraq was a step in the right direction, most forces continued to implement very different practices from the emerging COIN doctrine. An example is Operation Swarmer in March 2006, conducted by the 101st Infantry Division (Air Assault) in and around Samarra, which was described as the largest air-assault operation to-date, but which

---

[736] Nancy M. Dixon, Nate Allen, Tony Burgess, Pete Kilner, and Steve Schweitzer, *Company Command: Unleashing the Power of the Army Profession* (Center for the Advancement of Leader Development & Organizational Learning, 2005).

[737] Austin Long, *Doctrine of Eternal Recurrence: The U.S. Military and Counterinsurgency Doctrine, 1960–1970 and 2003–2006* (Santa Monica, CA: RAND, 2008), 21.

[738] Ibid., 22.

swept through areas largely empty of insurgents.[739] Robert Komer spoke to this difference between doctrine and organizational practices in a 1972 diagnosis of the U.S. Army's performance in Vietnam, noting: "equally striking is the sharp discontinuity between the mixed counterinsurgency strategy which U.S. and GVN policy called for from the outset, and the overwhelmingly conventional and militarized nature of our response."[740] The reasons for which lie deep in the organizational culture of traditional militaries' penchant for high-intensity conflict, a culture that emphasizes large battles and maximum use of firepower, while also emphasizing friendly force protection measures leading to large bases separated from the population.[741] Some examples of practices matching doctrine existed, as U.S. SOF sought to follow COIN principles within their doctrinal Foreign Internal Defense (FID) mission. Throughout the country, small teams were embedded, or stood up Iraqi Army and police units, generally lived off the FOBs, and conductedg HUMINT-driven operations with their local Iraqi partners. However, overall, these efforts were too few, disconnected, and dispersed to truly pressure a shifting insurgent network, and with few exceptions, primarily focused on developing local ISF capability to conduct raids against insurgent threats.

As a fragmented implementation of doctrine would imply, operational methods used by U.S. forces also varied. The standard practice was large-scale cordon and searches for insurgents; while these usually featured Iraqi Army forces, they were short-duration operations that provided little enduring security, nor did much to gain local support.[742] As U.S. forces consolidated themselves even further onto FOBs, their only real presence in many areas was such large-scale operations, which promoted a vicious cycle in which insurgents were provided freedom of maneuver most of the time, and could flow back into areas and capitalize on local dissatisfaction with a heavy occupation presence. Caught between an increasingly level of deadly insurgent capabilities, such as

---

[739] Brian Bennett, "On Scene: How Operation Swarmer Fizzled," *Time*, March 17, 2006, http://www.time.com/time/world/article/0,8599,1174448,00.html.

[740] Robert W. Komer, *Bureaucracy Does Its Thing: Institutional Constraints on U.S.—GVN Performance in Vietnam* (Santa Monica, CA: RAND, 1972), 37.

[741] Long, *Doctrine of Eternal Recurrence*, 27.

[742] Kilcullen, *The Accidental Guerrilla*, 124.

IEDs, RPGs, and armored-piercing grenades and light-skinned vehicles, coalition forces were challenged just to maintain freedom of movement in many areas. As John Arquilla and Doug Borer describe, "American troops, laagered in for the most part on about three dozen large forward operating bases (FOBs), were necessarily slow to reach sites that had been attacked, predictable in their patrolling movements, and of little deterrent value."[743] Operationally, SOF focused on targeting enemy insurgent leadership and added the growing number of groups to target lists that had once been exclusively focused on Ba'ath Party leadership, or foreign regime elements (FRE). In many ways, SOF remained true to its core missions, with Army SF and Navy SEALS focused on partnering with small Iraqi units to fight at the local level and JSOTFs targeting senior leadership. Following the second offensive against Fallujah, these JSOTFs began pursuing the entire AQI network, and focused on capturing or killing foreign fighters and the elusive leadership. The brunt of this effort centered on the ERV, where AQI had insulated itself in several tribes, most notably the al-Rawi tribe. Efforts to deny AQI a sanctuary in the ERV, such as Operation Snake Eyes, were the first true counter-network operations conducted in Iraq, in which the focus extended beyond a single leadership figure.[744] These efforts dramatically increased pressure against AQI along the river valley, which forced most of their leadership out of the ERV and into the areas surrounding Baghdad.

The U.S.-led coalition began the war with every effort to provide for a high degree of information flow, with embedded media in nearly every unit participating in the invasion. Yet despite this open acceptance of media, as the coalition faced challenges, it appeared to be constantly on the defensive with respect to information strategy. In an open letter to President George Bush in January 2006, Joseph Collins, a former Bush administration official, predicted, "if our strategic communications on Iraq don't

[743] John Arquilla, and Douglas A. Borer, "Strategic Dimensions of the Iraq Conflict," in *The Three Circles of War: Understanding the Dynamics of Conflict in Iraq*, *The Three Circles of War: Understanding the Dynamics of Conflict in Iraq*, ed. Heather S. Gregg, Hy S. Rothstein, and John Arquilla (Washington, DC: Potomac Books, 2010), 181.

[744] Mark Urban, *Task Force Black: The Explosive True Story of the SAS and the Secret War in Iraq* (London: Little, Brown Publishing, 2010), 85.

improve, the strategy for victory will fail and disastrous consequences will follow."[745] Ironically, the radically changed environment in Iraq meant that where formerly satellite TV was forbidden, soon after the invasion, the country was flooded with satellite dishes and an information-starved society was inundated with media. In this atmosphere, one would have expected U.S. and coalition forces to make a major communications effort to educate the people of Iraq concerning the goals of the coalition forces and the transition to democratic rule. However, the United States seemed to have had no real outreach plan. Lt. Gen. Thomas F. Metz, former MNC-I commander succinctly stated:

> We are not consistently achieving synergy and mass in our strategic communications (consisting of IO, public affairs [PA], public diplomacy, and military diplomacy) from the strategic to the tactical level….The collective belief is that we lack the necessary skills, resources, and guidance to synchronize IO in order to achieve tangible results on the battlefield…..In some respects we seem tied to our legacy doctrine and less than completely resolved to cope with the benefits and challenges of information globalization.[746]

Overall, the U.S.-led coalition displayed a dramatic disconnect between stated strategies and actual actions, which demonstrated a lack of meaningful information strategy. An emphasis on withdrawal, when Iraqis wanted security, an emphasis on freedom, when Iraqis wanted justice, and a general display of actions that undercut U.S. efforts "…indicates the administration [U.S.] lacks the flexibility that is an absolute requirement to deal with a networked, agile enemy."[747]

2. AQI Network Response

The Iraqi insurgency resulted from a complex combination of factors, some of which were both foreseen and preventable.[748] Yet, regardless, the threat it posed to

---

[745] Joseph Collins, "An Open Letter to President Bush," *Armed Forces Journal* (January 2006) http://www.armedforcesjournal.com/2006/01/1403023/.

[746] LTG Thomas F. Metz, "Massing Effects in the Information Domain: A Case Study in Aggressive Information Operations," in *Ideas As Weapons: Influence and Perception in Modern Warfare*, ed. G.J. David Jr. and T.R. McKeldin III (Washington, DC: Potomac Books, 2009), 266.

[747] Thomas X. Hammes, "Information Operations in 4GW," in *Global Insurgency and the Future of Armed Conflict*, ed. Terry Terriff, Aaron Karp, and Regina Karp (New York: Routledge, 2008), 203.

[748] Shultz and Dew, *Insurgents, Terrorists, and Militias*, 250–252.

coalition forces and an emerging Iraqi government presented difficulties that seemed insurmountable. The primarily Iraqi-led popular insurgency grew in scope and diversity to include numerous insurgent groups. AQI was the most catalytic and infamous of the groups, recognized as a part of the Al-Qaeda network by Osama bin Laden in December 2004.[749] AQI's violent tactics, use of information operations, and quest for organizational control combined to make it a unique opponent. The sophisticated nature of AQI's tactics, its ability to connect with global jihadist networks, and its funneling of foreign fighters into the insurgency led to its designation as a primary threat to coalition efforts.

Initially, AQI sought to achieve control of western Iraq, primarily the ERV, and use it as a safe haven from which to launch attacks against coalition forces and the emerging Iraqi government. This safe haven required the support of the tribal Sunni population, which was recognized by AQI as necessary for concealing its growing foreign composition.[750] Forming ties with the Sunni populace provided access to information on local conditions and a base of popular support for the jihadist struggle. Zarqawi sought to build a network of areas throughout the country that would support such activity, claiming early in the war that "we have taken possession of growing numbers of locations, praise be to God, to be base sites for brothers who are kindling [the fire of] war and drawing out the people of the country into the furnace of battle so that a real war will break out, God willing."[751] His strategy consisted of two main components focused, not on the U.S. occupation forces, but on the "underlying sectarian divisions in Iraqi society," as well as an unyielding salafist ideology.[752] However, AQI's partnership with the Sunni tribes in al-Anbar was short lived and their coercive practices provided the

[749] Hashim, *Insurgency & Counter-insurgency in Iraq,* 143.

[750] Fishman, *Bombers, Bank Accounts, and Bleedout,* 5–6.

[751] al-Zarqawi, *Signed Zarqawi Letter seized in 2004,* 244.

[752] Fishman, "After Zarqawi," 24.

motivational roots for Sunni tribal resistance, beginning as early as 2005.[753] Further, dramatic targeting efforts by coalition SOF throughout the ERV pressured AQI, forcing it in turn, to resort to more heavy-handed methods to maintain control. As Marine Major General John F. Kelley described, "over time, however, it [AQI] overplayed its hand and wore out its welcome by forcing an extreme Islamic agenda on a generally secular and very tribal culture. Al-Qaeda's campaign evolved from assistance, to persuasion, to intimidation, to murder in the most horrific ways, all designed to intimidate Anbari society…."[754]

By 2006, heavily pursued by coalition SOF in the ERV, AQI consolidated control in key areas surrounding Baghdad, such as Yousifiyah, Abu Ghraib, and Tarmiyah, and embarked on a campaign for control of the "Baghdad belts." The focus of these attacks was against targets in Baghdad, recognizing its primary role as a hub of media operations. In addition, it sought to maintain control in Ramadi and Mosul, viewing them as strategic sites for Al-Anbar and Ninewah Provinces, respectively.

As an organization, AQI expanded from its initial core of Tawhid operatives by starting small, connected, cells throughout the country, initially gaining local support for its efforts to oppose the U.S. presence. These cells were spread into nine regions within northern and western Iraq, headed by notable leaders, such as Umar Bazyani in Baghdad,

---

[753] Perhaps the best overall study of the reasons for AQI's decline with respect to its Sunni tribal relationships is found in Sean McClure, "The Lost Caravan: The Rise and Fall of Al Qaeda in Iraq, 2003–2007" (Master's thesis, Monterey, CA: Naval Postgraduate School, 2009). Other resources include Gary W. Montgomery and Timothy S. McWilliam's two volume compilation of interviews from both the U.S. and Iraq perspective, the most telling of which is *Al-Anbar Awakening, Volume II: Iraqi Perspectives, From Insurgency to Counterinsurgency in Iraq, 2004–2009* (Washington, DC: Government Printing Office, 2009); Najim Abed Al-Jabouri and Sterling Jensen, "The Iraqi and AQI Roles in the Sunni Awakening," *Prism* 2, no. 1 (2010); MAJ Neil Smith and COL Sean MacFarland, "Anbar Awakens: The Tipping Point," *Military Review* 88, no. 2 (March/April 2008): 41–52.

[754] MG John F. Kelley, as quoted in Gary W. Montgomery and Timothy S. McWilliams, ed. *Al-Anbar Awakening, Volume II: Iraqi Perspectives, From Insurgency to Counterinsurgency in Iraq, 2004–2009*, (Washington, DC: Government Printing Office, 2009), viii, http://smallwarsjournal.com/documents/anbarawakening2.pdf.

Abu Talha in Mosul, and Abu Nawras al-Faluji in Fallujah.[755] It did this by forming ties with local tribes through a variety of ways, including offering training assistance, bribery, and intermarriage within the tribal structure. Although effective in securing initial support, the coercive presence and strict salafist practices of AQI offended much of the tribal Sunni population. As the senior sheikh of the Albu Mahal tribe stated after the six months of AQI control of Fallujah, "…the second one [Battle for Fallujah] changed the view and the vision of the people against al-Qaeda, because they started to realize who al-Qaeda are. Al-Qaeda are people who kill, demolish houses, rape people, so the people started to change their view of the resistance."[756] Within the AQI organization, a core group of foreign jihadists provided leadership and direction, establishing connections with a dispersed network of regional cells. These cells were headed by "Emirs," which in some cases, were promoted into those positions based on the number of people they had killed.[757] At the higher leadership levels, AQI maintained a tight cadre of foreigners, providing a semblance of hierarchy, and emulating the larger al-Qaeda core leadership structure, which functions as a command cadre.[758] While descriptions of such structure use terms like chain-of-command and hierarchy, the levels of connectivity within the organization creates a larger network, as evidenced by AQI's regional connections, flexibility, and information flow. In this sense, AQI functions like a core-periphery network, maintaining a central leadership structure, but forming connections and providing autonomy to dispersed cells to conduct operational activity. In an effort to broaden its appeal following the December elections of 2005 and reconnect with its diminishing Sunni base of support, AQI formed the "Mujahedeen Shura Council" (MSC),

---

[755] Brisard, *Zarqawi*, 137; "Copy of Security Report on Al-Zarqawi, Ansar al-Sunnah Groups," from "Al-Zarqawi Was the mastermind of the attack on Dr. Barham," published by Iraqi independent weekly newspaper, *Awena*, February 28, 2006; derived largely from the "Confession of Umar Bazyani to Iraqi Security Forces, http://www.redorbit.com/news/international/415538/copy_of_security_report_on_alzraqawi_ansar_alsunnah_groups_/index.html.

[756] Despite these initial reactions to AQI's brutal practices and strict ideology, it would take the proper circumstances for the tribes to truly stand up to AQI. Sheikh Sabah al Sattam, as quoted in Montgomery and McWilliams, ed. *Al-Anbar Awakening, Volume II*, 143.

[757] Hashim, *Insurgency & Counter-insurgency in Iraq*, 144.

[758] Gunaratna and Oreg, "Al-Qaeda's Organizational Structure and its Evolution," 1045, 1065.

in January 2006.[759] The concept behind the MSC appeared to recreate some of the initial unity of purpose during the early stages of the war, such as the early siege of Fallujah when most of the mujahedeen factions were proud to conduct joint operations with AQI. An indicator of this effort is the appointment of an Iraqi, "Abu Omar al-Baghdadi," as the titular head of the MSC, allowing Zarqawi and other key foreigners to move out of spotlight.[760] With Zarqawi's death in June 2006, and his replacement by another foreigner, Abu Ayyub al-Masri, an Egyptian jihadi with field experience since the 1980s, AQI again sought further integration with Sunni insurgents. After a period of internal reorganization, on October 15, 2006, the MSC spokesman. al-Baghdadi, announced the formation of the "Islamic State of Iraq" (ISI).[761] Each of these efforts reflected an overall strategy of portraying the AQI organization as part of a larger, inclusive struggle.

While utilizing guerrilla-like raids and ambushes against U.S. and coalition forces, AQI quickly adopted a larger doctrine emphasizing terror attacks that would have a more significant effect than just military losses. This doctrine was largely based on intimidation using terror attacks that utilized suicide bombers and vehicle-borne IEDs (VBIEDs), kidnappings and executions, and assassination of Iraqi figures and coalition supporters.[762] Realizing that over time the Sunni population might gradually be drawn into the growing ISF and co-opted by coalition promises, Zarqawi's strategy was to provoke the Shi'a into a fury, and thereby, create a threat that would rally the Sunni's under AQI's banner:

> In our view they [Shi'a] are the key element of change. I mean that in making them our targets and striking at the heart of [their] religious, political, and military structures we will trigger their rage against the Sunnis…[forcing them] to bare their fangs and reveal the sly rancor that drives them from deep within. If we manage to draw them onto the terrain of partisan war, it will be possible to tear the Sunnis away from their heedlessness, for they will feel the weight of the imminence of

[759] Evan F. Kohlman, "State of the Sunni Insurgency in Iraq," 3, http://www.nefafoundation.org/index.cfm?pageID=24.

[760] Kenneth Katzman, "Al-Qaeda in Iraq: Assessment and Outside Links," *CRS Report RL32217*, August 15, 2008, 12, http://www.fas.org/sgp/crs/terror/RL32217.

[761] Kohlman, "State of the Sunni Insurgency in Iraq," 4.

[762] Malcolm W. Nance, *The Terrorists of Iraq* (Internet Publishing, www.booksurge.com, 2007), 274.

> danger….Most of the Sunnis are aware of the danger these people represent, distrust it, and know what would happen if they let them gain power.[763]

This overall strategy promoted an offensively focused doctrine that used terror tactics to generate significant effects against the Shi'a population, or symbolic targets, and/or generate significant media coverage. In addition, AQI clearly demonstrated the ability to swarm in ways that provide a significant challenge to combat. Using suicide bombers and VBIEDs, AQI conducted terror operations that featured multiple attacks simultaneously across Baghdad. These attacks were designed to intimidate the local population, portray the Iraqi and coalition forces as incapable of providing security, and generate significant media coverage. For example, in July 2005, 27 civilians were killed when a suicide attack struck U.S. soldiers passing out aid, and another 25 killed when 10 suicide bombers struck targets in coordinated attacks in Baghdad.[764]

Operationally, AQI cells conducted terror attacks within this rough doctrinal framework, striking coalition forces with ambushes and raids. Drawing on past jihadist experience, its organizational framework, and the asymmetric nature of the fight in Iraq, AQI (and the greater Iraqi insurgency) featured raiding as a central operational concept. In many ways, these surprise attacks had come full circle because they had been a core aspect of an original Bedouin way of fighting that originated in Arabia. Such tactics were well suited to rural areas, but were also adapted to fighting in urban areas, as the fierce fighting in the complex urban terrain of Fallujah demonstrated. As Richard Shultz noted, "these highly unpredictable, loosely networked, and adaptive groups of guerrillas and terrorists come together to strike and then disperse with considerable skill. They epitomize the urbanization of conflict today."[765] AQI also emphasized high-profile VBIED attacks, and this weapon became a hallmark ingredient of AQI's campaign of

---

[763] al-Zarqawi, *Signed Zarqawi Letter Seized in 2004*, 256.

[764] Dan Eggen and Scott Wilson, "Suicide Bombs Potent Tools of Terrorists," *Washington Post*, July 17, 2005, A1, http://www.washingtonpost.com/wp-dyn/content/article/2005/07/16/AR2005071601363.html.

[765] Shultz and Dew, *Insurgents, Terrorists, and Militias*," 254.

bombings and deadly mass attacks.[766] The use of VBIEDs provided a stealth capability for devastating attacks displaying potent economy of force, even when guided by a suicide driver. An early 2005 assessment of Salafi Web sites found 154 names of foreign jihadist fighters that had died in Iraq, with 33 of those reportedly "martyred" while executing suicide attacks.[767] Another report estimates that of the 440 suicide attacks occurring between March 2003 and August 2006, at least 30 percent were AQI operations.[768] In addition to providing the spark that started the Sunni-Shi'a civil war inside Iraq, AQI also became its chief executioners. Small cells conducted kidnappings, executions, and assassination of those who opposed its efforts at control. During the vicious sectarian struggle for control of Baghdad neighborhoods, AQI cells would literally kidnap entire families from their homes, execute them and dump the bodies in the streets. These attacks provoked a vicious Shia response, as "death-squads" led by Shia militias, retaliated in kind. AQI drew financial support from a variety of sources, including donations from both internal and external sources. Further, AQI generated increasingly used criminal operations to generate larger amounts of money inside Iraq, a component that grew to become a significant operational endeavor. Much of their bankroll was gained through physical extortion of Iraqi business and U.S.-funded contractors, a practice so pervasive it touched nearly every enterprise, which demonstrated the extensive operational efforts. Further highlighting the abilities of fighting networks, AQI displayed an ability to innovate through adaptive tactics:

> As a result, the astute enemy has continued to outpace us in the use of actions combined with information and backed up by more actions. Kidnappings followed by video tapes of beheadings are designed to shock and strike fear into the hearts of soldiers and civilians alike. Terrorist acts that target anyone working with U.S. Coalition forces are aimed at preventing such cooperation. Destruction of pipelines is designed to give the population of Iraq the idea that the Coalition cannot secure anything. IEDs are aimed at making the U.S. forces, in particular, 'heavy up,' and

766 Nance, *The Terrorists of Iraq*, 287.

767 Shultz and Dew, *Insurgents, Terrorists, and Militias*," 237.

768 Mohammed M. Hafez, "Martyrdom Mythology in Iraq: How Jihadists Frame Suicide Terrorism in Videos and Biographies," *Terrorism and Political Violence* 19, no. 95 (2007): 97–98.

> avoid contact by staying in their base camps. Interestingly enough, these IEDs are frequently videotaped and put up on blog sites for the media to pick up in the nightly news.[769]

AQI's operational efforts display a strong information component, and its overall campaign reflects an understanding of information strategy. As Lt. Gen. Metz stated, "further complicating our efforts in the information domain is the fact that we are facing an adaptive, relentless, and technologically savvy foe who recognizes that the global information network is his most effective tool for attacking what he perceives to be our center of gravity: public opinion, both domestic and international."[770] AQI's information strategy sought to achieve three broad objectives: first, rally Sunni support and recruit for their brand of insurgency; second, demonstrate to al-Qaeda that it was capable of carrying the torch of jihad in Iraq; and third, mobilize public opinion in the West against the occupation. The tools available to them included advanced digital imaging, broadband Internet connectivity, satellite communications, all of which could be accessed from nearly everywhere on the modern irregular battlefield. AQI quickly demonstrated the power of information in modern conflict, which validated the claim that "the camera has more importance than the weapon, video is worth more than a thousand sermons."[771] As an example of this importance, one of AQI's most critical posts was the "Media Emir," held by Abu-Maysara al-Iraqi for some time. Most of AQI's operations have an information component to them, from an IED attack to a large-scale suicide bombing. The "flash-to-bang" between a bombing and its posting on the Internet was, in many cases, just minutes. In addition, many operations, most notoriously kidnappings and filmed executions are planned and conducted for the express purpose of sending a message. Beginning with the execution of Nick Berg in May 2004 and lasting until the killing of Zarqawi, such executions formed a critical part of AQI's messaging, and provided one of the most effective ways of ensuring a terror threat is both "more horrible

---

[769] Richards (Ret.), Wilcox (Ret.), and Wilson (Ret.), "America in Peril," 120.

[770] Metz, "Massing Effects in the Information Domain," 266.

[771] Kenneth Roth, "The Wrong Way to Combat Terrorism," *The Brown Journal of World Affairs* (Summer/Fall 2007): 116.

and more credible."[772] In addition, his graphic use of beheading followed extensive efforts designed to communicate its legitimacy to the Muslim world. Combining such horrific, very real, actions that shocked audiences, with misleading information, such as the imprisonment and abuse of women in American jails, actually contributed to the "emotional" power of AQI's overall message.[773] Further, AQI's use of the Internet and a myriad of jihadist websites have a greater reach than most leading Arabic-language newspapers, and they promote the "truth" AQI wants its audience to see.[774]

Iraq Insurgency: 2003–2006				
	Organization	Doctrine	Operations	Information Strategy
U.S. Forces	*Traditional Hierarchy *Multiple Commands	*Combined Arms *Stability & Support focus *Mixed COIN	*Cordon and search *HVI Hunting	*Basic Propaganda *Formal Press Releases
AQI Forces	*Leadership Cadre *Numerous small cells *Highly connected *Popular support	*Swarming *Offensive Attacks *"Terror" Strikes	*IEDs *Suicide Operatives *Sparse Guerrilla action	*Constant Internet Presence *Shock Value of Attacks

Table 11. Evaluation of the 1st Phase of the Iraq Insurgency

[772] Martha Crenshaw, "The Logic of Terrorism: Terrorist Behavior as a Product of Strategic Choice," in *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, ed. Walter Reich (London: Cambridge University Press, 1990), 20–21.

[773] Napoleoni, *Insurgent Iraq*, 8–9.

[774] Daniel Kimmage and Kathleen Ridolfo, "Iraqi Insurgent Media: The War of Ideas and Images," *Central European Journal* 1, no. 2 (November 2007): 11, http://kms2.isn.ethz.ch/serviceengine/File/RESSpecNet/99882/ipublicationdocument_singledocument/BEB76AD2-D23D-4E2A-9A1D-D15102.

3. Analysis of Counter-Network Framework

a. Offensive Swarming

Critical components of offensive swarming are surprise, operational tempo, and pulsing. Each of these elements requires having precise intelligence, or information about where targets are located, patience to collect intelligence in view of long-term effects, and the ability to strike without revealing oneself. The majority of U.S. forces simply lacked intelligence about the insurgency, and in the early days of the conflict, even denied that it existed. The daunting task of pursuing an irregular enemy in a foreign culture led to large-scale operations that attempted to deny areas to the enemy, cordon-and-search missions for "suspected" insurgents, and sweeps for caches and IED-producing materials. While these efforts were conducted with the best of intentions, its largely conventional nature had little overall effect on elusive enemy networks. While offensive in nature, the attacks on Fallujah provide an example of AQI's ability to dodge even the heaviest of blows; although deciding to fight, many fighters and most leadership dispersed to other locations. Even SOF missions, largely intelligence-driven, aimed primarily at capturing key leaders, or high-value individuals (HVIs) within the AQI network, were a legacy from the leadership targeting of the FRE. It would not be until several years into the war that SOF elements would transition to effective offensive swarming.

b. Illumination

Displaying a dramatic deficit of cultural understanding and awareness of the nature of the irregular struggle, U.S. forces largely lacked both the insights and the capabilities required for successful illumination of the AQI network. As one U.S. intelligence officer said, "this lack of understanding has chased us since our haphazard beginnings of the war to the fitful, reactive, and stodgy manner that we prosecute the war

today."[775] The complex network of insurgent groups, with different compositions, motivations, and aims all served to complicate efforts to further understand the enemy threat, let alone isolate the most deadly group. As Bing West wrote, "American and Iraqi soldiers have no idea who their enemies are. In the rare instances when insurgents are actually captured, American rules and a corrupt Iraqi judicial system have converged to ensure that most are released…."[776] Most efforts at illumination were focused on enemy operational activity once an attack occurred, an IED exploded, or kidnapping occurred, but was usually limited to addressing that specific incident rather than using that event as a lever for further insights into the network. Local collection efforts were largely confounded by the lack of skilled HUMINT practitioners throughout the force, and infiltration efforts a bridge too far.[777] Following the revelations of Abu Ghraib travesties in April 2004, much of the coalition recoiled from efforts to conduct meaningful exploitation, and detainees were shuttled to larger holding facilities, and in many cases, quickly released. In fact, this recidivism came to be seen as a symbol of the larger Sisyphean struggle U.S. forces faced, as "the net result is that more than 80 percent of those detained are released within six months and usually in less than one month."[778] While many of those released were obtusely detained during large-scale sweeps, releases also included hard-core fighters. These shortcomings, combined with a lack of information management and sharing, or a lack of organizational fusion, served to short circuit illumination efforts. Multiple factors led to an ignorance of "…one of the most fundamental axioms of counterinsurgency warfare: an insurgency cannot be defeated if the enemy cannot be identified."[779]

---

[775] LTC George J. Stroumpos, "Clouding the Issue: Intelligence Collection, Analysis, and Dissemination during Operation Iraqi Freedom," in *Ideas As Weapons: Influence and Perception in Modern Warfare*, ed. G. J. David Jr. and T. R. McKeldin III (Washington, DC: Potomac Books, 2009), 251.

[776] Bing West, "Iraq and a Singular Information Failure," in *Ideas As Weapons: Influence and Perception in Modern Warfare*, ed. G. J. David Jr. and T. R. McKeldin III (Washington, DC: Potomac Books, 2009), 221.

[777] Richards (Ret.), Wilcox (Ret.), and Wilson (Ret.), "America in Peril," 124.

[778] West, "Iraq and a Singular Information Failure," 225.

[779] Ibid., 222.

c. Information Disruption

Information disruption capability and activities flows from a proper overall information strategy, which, as discussed previously, was largely lacking in early U.S. efforts. AQI's overall purpose was to conduct jihad against the U.S. occupation and deny Shi'a control in Iraq, and many U.S. actions contributed to reinforcing this narrative. In addition, even U.S. statements reinforced this message, as displayed by a White House statement that "we're dealing with some foreign terrorists, who are coming in from outside the country to fight what they believe is an extremely important jihad."[780] Efforts to deny, or channel, AQI's information flows were largely non-existent due to its access to multiple avenues of communication, most notably the Internet. Clearly, some collection efforts were in place, but for most of the early years of the war, these efforts had little focus. Most deception efforts remain classified, but with few other noticeable information disruption efforts, it is logical to assume that they were rarely incorporated.

d. Fusion

Fusion is primarily about shared intent that creates organizational connectivity and doctrinal synchronization. While U.S. forces in Iraq were clear on their primary task—to defeat Saddam and overthrow the Ba'athist Regime—once that was accomplished most of the strength of intent was lost. The primary reasons for a weakened intent were a lack of shared doctrinal understanding, mixed messages about how the war was being fought, and what the future held for U.S. forces. Notably, even into mid-2006, many U.S. forces were preparing for withdrawal and saw transitioning most of their efforts to ISF as the way ahead.[781] Given the lack of overall shared strategy, units shared little connection throughout the country and were primarily focused on maintaining an "over watch" status for their respective areas. SOF, while developing their own internal

[780] The White House, "Interview of National Security Advisor by KXAS-TV, Dallas, TX," November 2003.

[781] Kilcullen, *The Accidental Guerrilla*, 112–113.

systems for meshing operations and intelligence actives, were still largely focused on unilateral targeting, working with other forces where required, but not in an integrated fashion.

E. THE IRAQ INSURGENCY: 2006–PRESENT

The second phase of the Iraqi conflict witnessed significant shifts and the gradual assumption of control by U.S. and Iraqi forces. This shift, while dramatic, had multiple antecedents, the most significant of which began in 2006, but whose full effects were not realized until more than a year later. The most significant of these antecedents was an increase in SOF's precision targeting of AQI, the horrific sectarian violence instigated by AQI, and the Awakening movement by the Al-Anbar tribes.

By early 2006, SOF efforts against AQI in the ERV resulted in an AQI shift towards a strategy of surrounding Baghdad by staging in the areas encircling Baghdad, or it's "belts." Baghdad, with its large population and densely vegetated surrounding regions, provided a better safe haven than the narrow corridor of the ERV. Further, by concentrating its attacks in Baghdad, AQI was able to maximize its information effects, and gained considerable coverage with near daily devastating bombings throughout the capital.

Following the Samarra mosque bombing in February 2006, Shi'a reprisals against Sunnis brought the bloodletting that AQI's strategy sought. In the midst of U.S. withdrawal discussions, Iraq was suddenly pitched into a massive sectarian confrontation, as Kilcullen explained:

> During the rest of that year, an immense tide of blood washed over Iraq. Large parts of Baghdad were 'ethnically cleansed'; entire populations were killed and driven out. Hundreds of Iraqis died every week—Shi'ites in AQI and insurgent terrorist attacks, Sunnis in death squad executions by Shi'a communitarian militias retaliating for those attacks.[782]

As violence grew dramatically, reaching horrific proportions in the winter of 2006–2007, the landscape of Baghdad and surrounding areas slowly changed. Shi'a militias, many in

[782] Kilcullen, *The Accidental Guerrilla*, 125.

ISF employment, actually gained the upper hand against AQI and the Sunni population was the ultimate loser as entire neighborhoods were driven out. Although part of Zarqawi's plan, the Shi'a violence he provoked led to a loss of control of large areas of Baghdad, these internal struggles, combined with aggressive targeting of AQI, resulted in the loss of once strongly held AQI neighborhoods and regions.

A significant factor in breaking AQI's stranglehold, and reversing the momentum of the conflict was the *Sahwah*, "Awakening," of the Al-Anbar tribes. This awakening signaled a dramatic overt conflict between AQI and the Sunni tribes in the western province. Origins of this conflict appeared earlier, as the first evidence of strains between Sunni tribal leaders and AQI was the fighting that occurred beginning in May 2005, between tribal leaders in Husaybah and Al-Qaim. While tension existed between some tribes and AQI, overall, the strained relationship continued due to AQI's violent control, and the tribes' vacillation about firmly picking sides between AQI and a Shi'a dominated government. Increasingly coercive local actions by AQI, such as the mistreatment of the daughter of the Albu Jassim tribe and the brutal execution by beheading of Sheikh Abu Ali Jassim of the Anbar People's Council, provided the sparks that ignited the awakening, and were used by tribal leaders to rally support.[783] The leading spokesman for the Anbari tribal coalition resulting from the awakening, the Anbar Salvation Council (ASC), was Sheikh Abdul Sattar Abu Risha who defiantly spoke out against AQI. Having lost his father and three of his brothers to fights with AQI, and with a "gangster" background, he willingly became the front man for the awakening, declaring war against AQI in September 2006.[784] The partnership that resulted between Col. MacFarland's 1/1 AD in Ramadi and the ASC sheikhs would provide the catalyst for contesting AQI in Ramadi, and then throughout Al-Anbar. Capitalizing on the growth of the Al-Anbar tribal militias securing their own region, U.S. commanders initiated a complimentary program,

[783] Sheikh Ali Hatim al-Assafi, as quoted in Montgomery and McWilliams, ed., *Al-Anbar Awakening, Volume II*, 109; Francis J. West, *The Strongest Tribe: War, Politics, and the Endgame in Iraq* (New York: Random House, 2008), 174.

[784] Although a lesser sheikh, Abul Sattar's bold willingness to declare war against AQI provided a charismatic figure for tribal leaders to rally around, but it also made him a leading target and he was assassinated by an IED near his farm in September 2007. Governor Mamoun Sami Rashid al-Alwani, as quoted in Montgomery and McWilliams, ed., *Al-Anbar Awakening, Volume II*, 155.

the Sons of Iraq (SOI) to put other local, part-time security forces in charge of securing other areas. These programs proved highly successful and essentially incorporated former insurgents providing local security, and drew fighters away from AQI with a paycheck.

By the end of 2006 and into early 2007, most senior U.S. officials were calling AQI the driving force behind the insurgency. On April 26, 2007, General Petraeus called AQI "probably public enemy number one," in Iraq. While several months later, MNF-I spokesman Brigadier General Kevin Bergner, stated that AQI was responsible for 80–90 percent of the suicide bombings in Iraq, and that its defeat was the main focus of U.S. operations.[785] Yet, over the course of a year, AQI forces were dramatically disrupted throughout the Baghdad belts, highlighted by the destruction of key leadership and operational capabilities. The primary factor in this effort was a JSOTF-led campaign that connected multiple organizations, units, and capabilities together in a combined targeting effort. This effort was driven by joint employment of a unique combination of intelligence and operational activity, enhanced by an integration of technological breakthroughs. As General David Petraeus stated in a September 2008, *BBC* interview, "in fact, the breakthrough is not any one technological capability or intelligence advance: it is the fusion of all of those."[786] The fusion of high levels of intelligence with experience and ground-level tactical understanding of the environment presented a powerful display of joint operations.

In January 2007, President Bush announced a new strategy for Iraq, built on a counter-insurgency focus developed by an advisory team, and which "surged" U.S. forces to key areas. These forces provided a critical component missing in much of the counter-insurgency efforts to date, local presence to ensure security. Following on the heels of the awakening and the relentless pursuit of AQI, these forces allowed for sustained local engagement and security with physical control of Baghdad's key sectors. More importantly than just forces, however, was the strategy that employed them in small units and emphasized their connection to the local population.

---

[785] Katzman, "Al-Qaeda in Iraq," 11.

[786] Urban, *Task Force Black*," 272.

By 2008, severely disrupted AQI elements were primarily focused further north, seeking to re-organize and establish safe havens in northern Iraq.[787] Simultaneously, the flow of foreign fighters and resources was shifted further north, and operational activity in Baghdad limited to increasingly infrequent, but notably spectacular, attacks. Special operations efforts with partner Iraqi forces were also developing into robust counter-insurgent capabilities throughout the country. This synchronized combination of special operations employment provided a unique capability that allowed coalition forces to regain control within Iraq, and begin the long process of transition to stability. In General Petraeus's testimony to Congress in April 2008, he stated that the SOI, coupled with "relentless pursuit" of AQI by U.S. forces, had "reduced substantially" the threat AQI posed.[788]

Within a year, violence fell dramatically in Iraq, and the death of numerous AQI leadership figures prevented AQI from regenerating. Further, intensive targeting systematically collapsed critical AQI infrastructure, such as its media operations and extortion-based financing. A prominent feature of this targeting was combined efforts with increasingly capable Iraqi forces, which led to numerous breakthroughs against the network, including the death of Abu Umar al Baghdadi and Abu Ayyub al-Masri in 2010.[789] In a larger sense, SOF employment supported the comprehensive counterinsurgency strategy, and did so by providing special operations expertise against a challenging opponent in an unprecedented manner. By the close of 2010, most observers were saying that AQI had been severely degraded, to the point that it no longer posed a significant threat to the government of Iraq.[790]

---

[787] Bill Roggio, "Coalition Targets Al-Qaeda in the Iraqi North," *The Long War Journal*, March 5, 2008, http://www.longwarjournal.org/archives/2008/03/coalition_targets_al.php.

[788] General David Petraeus, Testimony before four Congressional Committees, as quoted in Katzman, "Al-Qaeda in Iraq," 15.

[789] "U.S.: 2 of Al-Qaeda's Top Leaders Killed in Iraq," *CBS News*, April 19, 2010, http://www.cbsnews.com/stories/2010/04/19/world/main6410912.shtml.

[790] Bill Roggio, "Al-Qaeda in Iraq's Security Minister Captured in Anbar," *The Long War Journal*, December 1, 2010, http://www.longwarjournal.org/archives/2008/03/coalition_targets_al.php.

1. U.S. and Iraqi Counter-Network Fight

Just when it seemed that the levels of violence in the Iraqi insurgency were spiraling out of control, and possibly taking the entire country along, the trend began to change. Overall, the levels of violence "decreased about 70 percent from June 2007 to February 2008, a significant reduction from the high levels of violence in 2006 and the first half of 2007, a trend that continues to the present."[791] In a February 16, 2008 statement, Iraqi Prime Minister Nouri al-Maliki stated that AQI had been largely driven out of Baghdad.[792] The remarkable turn around in the Iraq conflict, as evidence by increasing security and a decrease in enemy-initiated significant actions (SIGACTS) since late 2007 may only be explained by a complex combination of factors.

[791] Derived from Multi-National Coalition-Iraq SIGACTS Reports, 2007–2009, http://www.globalsecurity.org/military/ops/iraq_sigacts.htm.

[792] Katzman, "Al-Qaeda in Iraq," 12.

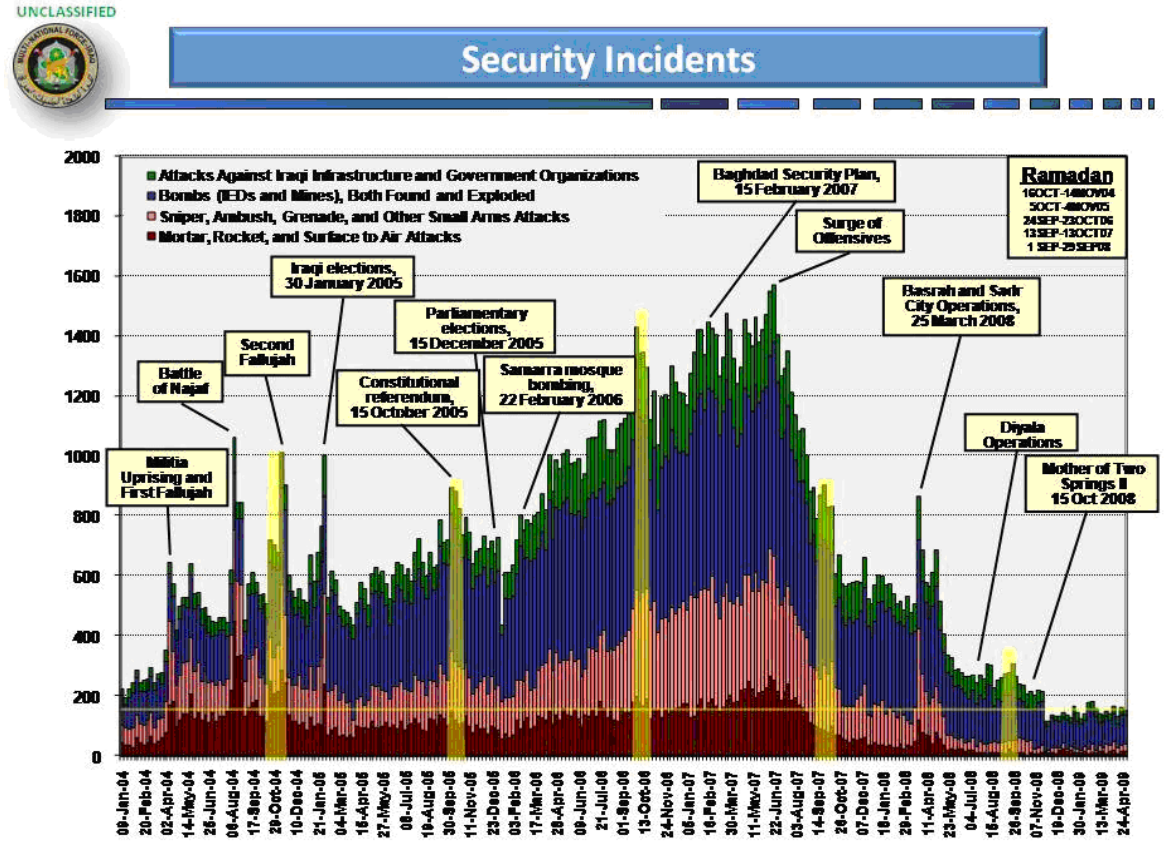

Figure 16. MNC-I Reported SIGACTS, January 8, 2004–April 24, 2009[793]

Numerous viewpoints exist, which have generated multiple theories to explain the reasons for the decline of the Iraqi insurgency. While many of these theories point to a specific cause, the story is much more complex, goes beyond key events, and requires an examination of the conflict, through multiple events, to the present. The full explanation of this change is beyond the scope of this thesis, but several notable factors include the following.

[793] SIGACTS Chart, http://www.globalsecurity.org/military/ops/iraq_sigacts.htm.

- The rejection of AQI by Al-Anbar tribal leadership, following vicious struggles for control.
- An increase in counter-network capability, primarily by U.S.-led coalition SOF, but facilitated by fusion cells and partnership with local conventional force commanders.
- A change in U.S. security strategy, which included multiple components, but the most effective was ensuring local security through small outposts and on-the-ground patrols that partnered with local Iraqi forces.[794]

In keeping with the scope of the study, this case focuses primarily on the last two factors, while including the Al-Anbar Awakening, and recognizing the dramatic shifts in the environment created by events, such as the sectarian bloodletting that changed large areas of Baghdad and surrounding provinces. In addition, multiple sources cite the interactive effect of the last two factors in allowing for these changes in the environment, for example, SOF targeting of AQI, which according to Col. MacFarland, "scared the bejeebers out of them," and provided a "critical enabler that gave the tribes breathing space," in and around Ramadi, further enabling the awakening.[795] This focus allows for the examination of the nature of the fight between the AQI network and those actively pursuing it, a fight that continued for years after the dramatic changes in 2006–2007. As General Petraeus stated in his September 10, 2007 address to Congress, "al-Qaeda is certainly not defeated; however it is off balance and we are pursuing its leaders and operators aggressively….These gains against al-Qaeda are a result of the synergy of actions by: conventional forces to deny the terrorist sanctuary; intelligence, surveillance, and reconnaissance assets to find the enemy; and special operations elements to conduct targeted raids. A combination of these assets is necessary to prevent the creation of a terrorist safe-haven in Iraq."[796]

---

[794] In a 2008 *Washington Post* article, Bob Woodward cites three main factors: 1) secret operations based on "collaborative warfare," 2) the al-Anbar Awakening, and 3) Muqtada al-Sadr ordering the Mahdi Milita stand down. Bob Woodward, "Why Did Violence Plummet? It Wasn't Just the Surge," *Washington Post*, September 8, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/09/07/AR2008090701847.html.

[795] Lamb and Munsing, "Secret Weapon: High-Value Target Teams as an Organizational Innovation," 30.

[796] Caraccilo and Thompson, *Achieving Victory in Iraq*, 180.

Organizationally, U.S. forces began to change and adapt to the increasing challenge of fighting the AQI network in mid-2006. These organizational changes were complemented by a surge of five U.S. Army and two Marine brigades, which was effectively the strategic reserve of the U.S. military.[797] This change increased the total number of forces in Baghdad from 17,000 to 40,000. These numbers would have an effect in nearly any city.[798] Yet, despite the numbers, organizational design and employment actually produced the dramatic effects leading to AQI's disruption. The Brigade Combat Team (BCT) concept brought significant flexibility with the capability to tailor units to respective areas and operating environments, as well as granted further autonomy to tactical commanders. Increasing levels of partnerships occurred as units became more integrated under a common strategic focus, and units of all types became increasingly focused on supporting the local commanders. "By the summer of 2007, the new Iraqi Assistance Group (IAG) commander, Brig. Gen. Jim Yarborough, recognized the need for unity of command for the BCTs. In an unprecedented and completely selfless move, he detached all MiTT [Military Transition Team] teams from the IAG's command and control to that of the land-owning commander."[799] This move placed oversight and advice for nearly all Iraqi forces, to include police and border patrols, under the operational control of the local commander, ensuring greater unity of effort. Further, and perhaps most significantly, the development of fusion cells promoted increasingly connected collection and operational efforts throughout the battlefield.[800] These intelligence collection and targeting cells provided a level of connection that spanned the entire theater of operations, which linked conventional, special operations, and coalition force targeting efforts. The fusion cells were consistently described as a major factor behind the declining violence in Iraq, with Joint Chiefs of Staff Chairman Adm. Michael Mullen stating that the cells produce intelligence leading to 10 to 20 captures a night in

---

[797] Bob Woodward, *The War Within: A Secret White House History 2006–2008* (New York: Simon & Schuster, 2008), 288.

[798] Ibid., 379.

[799] Caraccilo and Thompson, *Achieving Victory in Iraq*, 24.

[800] Multi-National Force-Iraq, "Fusion Cells to Help Locate Terrorists," *Combined Press Information Center*, December 14, 2006, http://www.usf-iraq.com/?option=com_content&task=view&id=8093&Itemid=21.

Iraq, "to me it's not just war-fighting now but in the future," Mullen said, "it's been the synergy, it's been the integration that has had such an impact."[801] Finally, organizations across the board sought to integrate with Iraqi forces at all levels, from national level counter-terrorism units, to local police and militias, such as the SOI. Even the once highly classified fusion cells were adapted and integrated with Iraqi forces, which provided an unparalleled level of information sharing.[802]

Doctrinally, the second phase of the war was driven by a coherent COIN doctrine both preached and practiced. The new Field Manual 3-24, *Counterinsurgency*, released in December 2006, provided an expanded manual, and both services also released complimentary manuals for small-unit leaders. The formative influence behind the manual was Gen. Petraeus, whose promotion to MNC-I commander, provided the leadership to synchronize doctrine across the theater. The primary tenet of this counterinsurgency doctrine was to protect the population by providing security, first and foremost. This approach was an offensive focus, requiring U.S. forces to engage the population and the enemy actively, rather than remain in a defensive posture in FOBs. As Thomas Ricks would write in his discussion of the Marine killings in Haditha in 2005, "indeed, another year would pass before the U.S. military would take the first step in counterinsurgency and begin to implement a strategy founded on the concept that the civilian population isn't the playing field but rather the prize, to be protected at almost all costs."[803] Further, such doctrine allowed other strategic efforts to occur, and by separating the population from other insurgents, it facilitated reconciliation with moderate factions, and allowed for increasing isolation and targeting of irreconcilables, most notably AQI. Doctrinal innovations resulting from bottom-up efforts greatly led to significant gains in the fight against AQI. The fusion cells provided an organizational

---

[801] Joby Warrick and Robin Wright, "U.S. Teams Weaken Insurgency in Iraq," *Washington Post*, September 6, 2008, 3, http://www.washingtonpost.com/wp-dyn/content/article/2008/09/05/AR2008090503933.html.

[802] Multi-National Force-Iraq, "Iraqi Fusion Cells Bring U.S., Iraqi intelligence-Gathering to New Heights," July 23, 2009, as listed on http://www.globalsecurity.org/military/library/news/2009/07/mil-090723-mnfi02.htm.

[803] Thomas Ricks, *The Gamble: General David Petraeus and the American Military Adventure in Iraq, 2006–2008* (New York: Penguin Press, 2009), 7.

flattening and connectivity, but also brought with them a doctrine focused on understanding the nature of the networked enemy. Doctrinal fusion is really the institution of collaborative systems, and, "having intelligence and operations working together in common space on a sustained basis produced persistent surveillance, improved discrimination, and better decision-making."[804] Rather than focus exclusively on capturing or killing AQI members, this doctrine sought to gain information on the network through a comprehensive targeting system. This doctrine evolved from targeting concepts generated as early as 2004, but reached new levels of effectiveness by 2006–2007, as it was increasingly understood and expanded upon. Incorporating aspects of network-style warfare, this doctrinal element provided an entirely new outlook on CT operations. The combination of both doctrinal elements provided a remarkable synthesis that both protected the population, but ensured a robust, precise targeting focus against the hard-core irreconcilables.

Operationally, the combination of a coherent strategy and doctrinal innovations resulted in an increasing security presence and enhanced targeting efforts against AQI. Small unit tactics received proper focus while cordon and search operations were intelligence driven, and employed against larger concentrations of AQI fighters. Combat outposts and the Joint Security Stations (JSS) became the operational paradigm, as platoon and company-sized units formed a network of outposts throughout Baghdad, initially, and then in contested areas. These outposts, manned 24/7 by U.S. and Iraqi security forces, provided constant security and interaction with local Iraqis to ensure a force that could find and fight AQI and other insurgents locally. In stark contrast to buttoned-up patrols along IED infested routes, local security emphasized dismounted patrolling and provided ground-level situational awareness. Patrolling in this manner allowed for U.S./Iraqi force integration, the ability to converse and interact with local Iraqi's, and the infantry flexibility to respond to urban and rural threats. Increasing connectivity and collaboration among SOF allowed for precision raids that dramatically increased in overall effectiveness, as multiple authoritative sources reported, "these

[804] Lamb and Munsing, "Secret Weapon: High-Value Target Teams as an Organizational Innovation," 1.

covert activities had a far-reaching effect on the violence and were very possibly the biggest factor in reducing it. Several said that 85 to 90 percent of the successful operations and 'actionable intelligence' had come from these new sources, methods and operations."[805] The most notable aspect of these operational methods, in addition to their overall focus on information collection, was a focus on disrupting the entire network through systematic targeting. Rather than attempt to capture just HVIs, this operational focus latched onto any visible node within the network, as one analyst described, "success against al-Qaeda in Iraq was achieved, in part, by targeting low-level fighters which generated the intelligence that allowed for the targeting of higher level commanders. This slowly tears the network apart from the inside, simultaneously forcing senior commanders to continually attempt to reboot defunct cells."[806] In a 2008 operation, which captured Abu Uthman, a legacy AQI member, "U.S. intelligence and defense officials credit the operation and its unusual tactics—involving small, hybrid teams of special forces and intelligence officers—with the capture of hundreds of suspected terrorists and their supporters in recent months."[807]

Coupled with increasing operational success, the U.S.-led information strategy displayed notable changes. The primary change was simply a common vision and shared intent, which provided U.S. forces in Iraq with a much-needed sense of purpose. As General Petraeus stated on his fourth day in command in Iraq, "we are in an information war, sixty percent of this thing is information," signally a dramatic shift in focus and encouraging commanders to engage in information strategy actively.[808] In addition, an emphasis on information engagement (IE, primarily in the form of tactical-level public affairs) led to generating timely products for media consumption and distribution and provided increased capability for generating reports and footage emphasizing the impacts

[805] Woodward, *The War Within*, 380.

[806] Jeffrey A. Dressler, *The Haqqani Network: From Pakistan to Afghanistan* (Washington, DC: Institute for the Study of War, 2010), 37

[807] Warrick and Wright, "U.S. Teams Weaken Insurgency in Iraq," 2.

[808] Ricks, *The Gamble*, 133.

of success.[809] Much of the information strategy during the initial crux of regaining stability focused on perception, and ensuring that the local Iraqis understood that the environment was changing. Moreover, these local perceptions were reinforced with news broadcasts that portrayed coalition successes. Complementing this effort was AQI's continued fixation on gaining attention through violent attacks, even after the bloodletting of the sectarian infighting left most Iraqis wearied from such repetitive violence, and craving basic stability. The latest version of Field Manual 3-0, *Operations*, reflects U.S. force lessons learned in Iraq, and highlights a shift towards embracing information employment as a fundamental aspect of irregular conflict. Its introduction reads, "informing the public and influencing specific audiences is central to mission accomplishment."[810] Reflecting such doctrine, the Multi-national Division-Baghdad (MND-B)'s also employed information operations (IO) "…adjusted to focus on informing the Baghdad population of imminent threats such as suicide vests and vehicle-borne improvised explosive devices (VBIED) attacks and disrupting AQI Support Zones."[811] Other aspects included using a "flashlight" approach to focus intense IO efforts along a particular operation, "highlighting security and essential services" to the Iraqi Government an ISF, as well as demonize AQI by focusing on its increasing violent acts.[812]

2. AQI Response

Despite the Sunni rejection in Al-Anbar, AQI aimed for increasing control and organizational supremacy over the insurgency in Iraq, as seen in violent clashes with other insurgent groups and the formation of its umbrella organizations, the MSC and ISI. The bitter struggle for control with other insurgent groups actually contributed to a spike in violence, as some groups, such as Islamic Army of Iraq (IAI) and the 1920s

---

[809] LTC Roger S. Galbraith, "Winning on the Information Battlefield: Is the Story Getting Out?" in *Ideas As Weapons: Influence and Perception in Modern Warfare*, ed. G. J. David Jr. and T. R. McKeldin III (Washington, DC: Potomac Books, 2009), 134.

[810] U.S. Department of Defense, Field Manual 3-0, *Operations*, vii.

[811] LTC Frank H. Zimmerman, "Attack, Attack, Attack, Information Operations," *IO Sphere*, Winter 2010, 10, http://usacac.army.mil/cac2/IPO/repository/iosphere.pdf.

[812] Ibid., 15–16.

Revolution Brigade, engaged in open fighting against AQI. Despite facing a common threat in the Shi'a death squads, these Sunni insurgents retaliated against AQI abuses, took back neighborhoods, and formed alliances with local U.S. forces.[813]

As it was pushed out of Baghdad, AQI sought to intimidate local populations further north, thereby creating safe-havens and buffer zones between populated areas and the desert wastelands it believed would allow its reconstitution. The dramatic suicide bombings, which totaled nearly 1,000 casualties, against rural villages in northern Diyala Province in July 2007, and in the Sinjar region of Ninewah Province in August 2007, served as clear messages—to support AQI, or die, to the locals in the area.[814] However, by displacing to these primarily rural areas, AQI became increasingly easier to find and target, despite its efforts at coercing local popular support.[815]

While still attempting to maintain influence in Baghdad, AQI shifted its operations north to the city of Mosul, a hub in Ninewah Province that provided support to cells throughout northern Iraq. The political fight for control between Sunni Arabs and Kurds within Ninewah Province provide room for AQI to exploit. AQI's use of Mosul as a base of operation began in the early years of the war, but as AQI's freedom of maneuver became more constrained, it became more significant.[816] With the Al-Anbar tribes controlling nearly all of the ERV, AQI's foreign fighters were routed through the last remaining foreign fighter facilitation network in the northern al-Jazeerah desert, making Mosul and the northern Tigris River Valley (TRV) even more critical. Still, despite desperate attempts to retain influence, a September 2009 Department of Defense

---

[813] Joshua Partlow, "For U.S. Unit in Baghdad, an Alliance of Last Resort," *The Washington Post*, June 9, 2007, Section A.

[814] The geographic location of these remote attacks differed from AQI's usual tactics of suicide bombings in large urban areas. The bombing in Qahtaniya, near Sinjar, used four vehicles and is the second-largest casualty producing terrorist attack on record. Notably, coalition forces conducted a strike on a desert tent south of Sinjar in October 2007, which provided extensive evidence of AQI's foreign fighter facilitation through the region and its desire to maintain control of such areas. Damien Cave and James Glanz, "Toll in Iraq Bombing is Raised to More Than 500," *New York Times*, August 22, 2007; Stephen Farrell, "Around 150, Death Toll in Iraq Attack Among War's Worst," *New York Times*, July 9, 2007; Brian Fishman and Joseph Felter, *Al-Qaida's Foreign Fighters in Iraq: A First Look at the Sinjar Records* (West Point, NY: Combating Terrorism Center, 2007).

[815] Ricks, *The Gamble*, 174.

[816] Brian Fishman, *Dysfunction and Decline: Lessons Learned from Al-Qaeda in Iraq* (West Point, NY: Combating Terrorism Center, 2009), 24.

reported, "significant leadership losses and a diminished presence in most population centers…"[817] Internally, AQI realized its weakening state, and one captured document even provides a summary of lessons learned, including the following.

- Failure to Understand the Iraqi People
- Unreliable Smugglers in Syria
- Propaganda Created Unrealistic Expectations among Foreign Fighters
- Bureaucratic AQI Emirs Failed to Coordinate
- Tension between Foreign Fighters and Iraqi Members of AQI
- Suicide Bombers Changed Their Mind
- Too Many Leaders Diluted Command Structure
- Bureaucratic Stovepiping
- Poor Use of Financial Resources[818]

Overall, despite attempts to re-organize and integrate itself using Iraqi social networks, AQI found itself increasingly isolated, disconnected, and pursued. As Fishman noted:

> AQI's efforts failed, in no small part because the public and private efforts at conciliation [with other insurgent groups and tribal leadership] were inconsistent with AQI's continued tactical violence. Effective insurgent and terrorist campaigns depend on tight coordination between political goals, tactical violence, and strategic communications.[819]

Despite publicly declaring the ISI cabinet in April 2007, to feature its Iraqi "cabinet ministers," pressure against the AQI organization led to a smaller, more clandestine leadership core.[820] The dispatching of senior al-Qaeda figures to assist in AQI's expansion evidenced greater affiliation with core Al-Qaeda leadership, largely due to long-standing relationships between al-Masri and Zawahiri, and efforts to regain control of the Iraqi insurgency. Most notable was Abu Hadi al-Iraqi, a former Iraqi Army officer

---

[817] U.S. Department of Defense, "Measuring Stability and Security in Iraq," September 2009, as cited in John Rollins, *Al Qaeda and Affiliates: Historical Perspectives, Global Presence, and Implications for U.S. Policy*, R41047, (Washington, DC: U.S. Congressional Research Service, February 5, 2010), 13.

[818] Harmony Database Document: NMEC-20080612449, as compiled in Fishman, *Dysfunction and Decline*, 16–20.

[819] Fishman, *Dysfunction and Decline*, 11.

[820] Kohlman, "State of the Sunni Insurgency in Iraq: August 2007," 5.

and Afghanistan veteran who served as a trusted al-Qaeda military operations leader for a significant period of time.[821] Other senior leaders included Mehmet Yilmaz (Khalid al-Turki) and Mehmet Resit Isik (Khalil al-Turki), and Turkish fighters with Afghanistan experience who were killed by coalition forces in June 20007.[822] Yet, regardless of their attempts to shore up the organization with experienced personnel, AQI continued to face dramatic losses, which exacerbated leadership problems. The Sunni tribal rejection, and AQI's increasingly bitter infighting with other insurgent groups, also further inflamed organizational issues, primarily the integration of foreign fighters into the network. As Brian Fishman states, "ultimately, those problems became so important that, according to a document captured in 2008, al-Qa'ida's leadership made the strategic decision to reject foreign fighters trying to enter Iraq."[823] Increasing pressure resulted in reduced communication throughout the network, as the "postal service" and other forms of communication were disrupted or increasingly compromised by tribal and insurgent differences.[824]

Doctrinally little changed for AQI from 2006 onward, although the formation of the ISI and its attempt to gain control over the Sunni insurgency reflect its most notable strategic aspect. The attacks against Shi'a population targets declined more due to a lack of access than a change of doctrine. The doctrinal hallmark of AQI's offensive terror remained massive suicide bombings, which were designed to produce large-scale civilian casualties, as evidenced by the attacks in northern Iraq in 2007. Terror bombings continue in Baghdad, although relatively infrequently, and it appears that the Iraqi security and intelligence apparatus is gaining capability, and often rapidly capturing those responsible.

---

[821] Katzman, "Al-Qaeda in Iraq," 17.

[822] Kohlman, "State of the Sunni Insurgency in Iraq: August 2007," 8.

[823] Damages to the foreign fighter facilitation network also likely contributed to this decision. Fishman, *Dysfunction and Decline*, 16.

[824] Fishman, *Dysfunction and Decline*, 15.

Operationally, AQI continued its campaign of intimidation through bombings and raids against U.S. and Iraqi outposts. In addition, the summer of 2008 saw a noticeable spike in targeted assassinations of Iraqi officials, many of whom were killed with the use of magnetic "sticky-bombs," which could be easily emplaced on the target's vehicle. As AQI faced increasing pressure and a loss of both internal resources and external support, it began to employ "organized" crime by using vast extortion networks to generate revenue.

The change in leadership from Zarqawi to al-Masri produced notable effects in AQI's information strategy. Whereas Zarqawi charismatically engaged in media operations, filming and conducting vicious beheadings and releasing propaganda videos, al-Masri assumed a lower profile. While this posture may have been safer in light of increased targeting pressure, it continued to marginalize the organization. This reluctance to engage contributed to a disconnect between public statements and AQI actions, suggesting that AQI's leadership did not understand the entirety of the backlash against it, which further reveals the increased difficulties in communication within the network.[825] Overall, AQI sought to regain lost ground by down playing the foreign status of its key leaders and instead utilized Iraqi leadership, most notably Abu Umar al-Baghdadi, as its public voice. Ironically, despite this effort to maintain a clandestine face, "AQI's failures were terribly transparent," and attempts to assert itself through bold propaganda worked to some degree but,

> …Iraq was different because AQI was not the only armed group with a media wing and a website. Iraq's tribes had internet campaigns as well, not to mention easier access to Arab satellite television media than did their jihadist counterparts. Not only was AQI starting to lose ground on the physical battlefield in Iraq, it was losing ground on the global media battlefield as well.[826]

[825] Fishman, *Dysfunction and Decline*, 12.

[826] Ibid., 10.

Iraq Insurgency: 2006–Present				
	Organization	Doctrine	Operations	Information Strategy
U.S. Forces	*Unity of Effort *Increased Collaboration *Fusion *Dispersed Small Units	*COIN Focused Strategy *SOF Swarming	*Outposts and Outreach *Local Population Security *Offensive Swarming	*Enhanced by AQI Terror *Consistent Narrative
AQI Forces	*"Iraqi" face *Numerous small cells *More clandestine	*Swarming *Offensive Attacks *"Terror" Strikes	*IEDs *Suicide Operatives *Assassinations	*Internet Presence *Weakened Narrative

Table 12. Evaluation of the 2nd Phase of the Iraq Insurgency

3. Analysis of Counter-Network Framework

The dramatic turn around that occurred in 2006–2007, and the subsequent pursuit and disruption of AQI throughout Iraq over the next 3–4 years, was largely a result of U.S. forces employing a synthesized strategy to protect the population, while simultaneously employing a robust counter-network approach. This later approach and the framework it employed resulted from innovations early in the conflict, but developed to fruition at a critical period to ensure AQI's subsequent defeat. This unified approach nested well within a robust counterinsurgency strategy, initiated beginning in 2007, which provided a common intent and purpose for U.S. forces. The overall focus on providing security for the population was absolutely consistent with, and complimented by robust, precise targeting efforts against irreconcilables, primarily AQI. The details of the targeting approach against AQI remains classified, but Christopher Lamb and Evan Munsing described three of its innovations, which were summarized as network-based targeting, fusion of improved all-source intelligence with operational capability, and integration of counterterrorist and counterinsurgency efforts.[827] Lamb and Munsing state,

[827] Lamb and Munsing, *Secret Weapon*, 1.

"…the new capability reportedly captured or killed enemies so fast it put their clandestine organizations on the defensive and gave population security measures a chance to shift public support to government forces," and make the case that the "…interagency teams used to target enemy clandestine networks were a major, even indispensible, catalyst for success."[828]

a. Offensive Swarming

Operationally, U.S. forces applied each aspect of offensive swarming against AQI. The integration of focused all-source intelligence collection and fusion provided the capability for dramatically increased operational tempo. Instead of conducting a single, deliberate raid as intelligence allowed, intelligence became the driving aspect of operations and even the slightest sign of AQI activity became a potential lead for further collection and targeting gains. Precision raids against AQI targets consistently achieved surprise, even more so when conducted in a rapid manner, with information from one mission leading directly to another target, and so on. The combination of conventional and SOF efforts led to a greater understanding of the local environment, which was crucial to effective pulsing. This understanding ensured the maximum potential gained through direct strikes, and often, large sections of the network were "illuminated" prior to operations to achieve larger effects and ensure that those effects were synchronized with local U.S. and Iraqi security efforts. Perhaps the most notable aspect of the operation that killed Zarqawi was not the AQI leader's death, but the following 450 raids in little more than a week.[829] Swarming occurred in the form of multiple 24/7 strikes against these illuminated nodes, operations that would continue until they achieved decisive effects. Further, the growing Sunni militias, most notably SOI, added considerable capability for rapid attacks against AQI that denied them freedom of movement through aggressive attacks wherever fighters concentrated.

[828] Lamb and Munsing, *Secret Weapon*, 5, 6.

[829] Urban, *Task Force Black*, 174.

b. Illumination

As previously outlined, efforts against a clandestine irregular force require considerable information, primarily focused on identifying whom and where the opponents are. The U.S. illumination efforts during the second phase of the war present an overall marked contrast to early efforts. A greater degree of security meant greater integration with the local population, and as a result, the overall understanding of social ties and tribal networks within Iraq grew considerably. The use of the F3EA cycle relied on interagency organization and gave primacy to intelligence collection, which dramatically changed the nature of targeting in Iraq by incorporating multiple assets and combining these with a greater awareness of local interaction. This cycle proved instrumental in "…charting the clandestine terrorist and insurgent cells and their immediate supporters to attack them, but also using all-source intelligence to reveal the local environment, its social networks, and key decision-makers and their motivations."[830] A significant aspect of this cycle was aerial surveillance, and in 2007, the number of drone reconnaissance aircraft operating in Iraq would increase tenfold, which furthered the ability to gain information, and complimented collection on the ground.[831] Moreover, this and other collection capabilities were making a significant difference at the tactical level, as a 1st Cavalry Division report stated, "synchronization of ISR/HUMINT/SIGINT (intelligence, surveillance, and reconnaissance/human intelligence/signals intelligence) has significantly reduced IED cells and threat."[832]

The sectarian violence and infighting between insurgent groups provided another type of operational activity, which forced visible, violent action that provided additional insight and areas of focus for further illumination. Infiltration, while still the most difficult aspect of illumination efforts, increased as well, with HUMINT providing a greater component due to a greater degree of local interaction and a sense that the tide had turned that motivated former AQI to turn against the violent activities of the group. Exploitation dramatically increased as well, which built on the overall degree of insight

[830] Lamb and Munsing, *Secret Weapon*, 1.

[831] Ricks, *The Gamble*, 192.

[832] Ibid., 193.

into the network. The detention system was structured to provide humane, efficient treatment; professional and effective interrogation techniques; and other options for fighters willing to provide information. Led by Maj. Gen. Douglas Stone, efforts the revamp the prison system paralleled the overall counterinsurgency effort to reduce the risk of prisons continuing as "…breeding ground for extremist recruitment."[833]

c. Information Disruption

Information disruption efforts capitalized largely on mistakes made by AQI, and more specifically, its use of indiscriminate attacks and brutal intimidation. While U.S. forces sought to negate AQI's violent media campaign, it retained its effectiveness until the larger population rejected it. While AQI's overall narrative changed as it attempted to embrace moderate Sunni Muslims, the damage had largely been done, and it was fairly straightforward to capitalize on its failing efforts. U.S. forces conducted effective channeling as well that overemphasized AQI's attack claims and highlighted the most horrific aspects of its violent tactics. In many ways, this channeling was more effective than outright denial, as most of the population either recoiled from such action, or had grown weary of the instability it promoted. The awakening tribes contributed to the overall information disruption efforts by conducting their own media campaigns against AQI and highlighted many of AQI's horrific acts. Their visible information efforts contributed to the growing perception of AQI's loss of popular support, and thus, reinforced U.S. efforts. Collection efforts against AQI grew in effectiveness, with the fusion of multi-source intelligence and increased presence on the ground. The former provided a means of disrupting technical sources, while the latter increasingly shut down the use of couriers and sympathetic support mechanisms. AQI's displacement from existing safe havens and operational areas in and around Baghdad forced increased communication, as it sought to re-establish itself, leading to better collection of all types.[834]

---

[833] Ricks, *The Gamble*, 195.

[834] Ibid., 174.

d. Fusion

At its core, fusion relies on a shared intent and purpose throughout the effort that united disparate agencies and groups into a unified team. U.S. forces understood the overall intent, and as a review of fusion cells in Iraq determined, the primary unifying element was "the sense of urgency, purpose and commitment to accomplish a mission."[835] Organizational fusion became a necessity in many parts of Iraq, and a notable example was the success enjoyed by Task Force Freedom in Mosul in 2005. While this success was a precursor to more robust integration in later years, the success it brought in Mosul foreshadowed the powerful role it would play. "The dynamic that made all this work was the personal involvement of individuals from each agency and their dedication to serving the task force and its mission, rather than their parent organization. New levels of interagency trust and combat-necessity gave birth to an unprecedented innovation: a national level intelligence team in direct support of a tactical task force."[836] Another notable example of fusion was provided by Col. MacFarland's 1/1 AD in Ramadi and SOF units when, "the brigade staff and SOF Task Force personnel in particular exchanged targeting files and prisoners and sat in on each other's targeting meetings, eventually leading to a 'seamless targeting process through liaison officers and the fusion center.'"[837]

F. CONCLUSION

The U.S. and Iraqi fight against AQI continues today, although it is widely believed that AQI is no longer in a position to threaten the government of Iraq. However,, despite the lack of media coverage, a bitter struggle continues, with AQI occasionally succeeding in devastating bombings against Iraqi civilians and political figures. As a case study, the fight against the AQI network provides numerous insights about how to counter fighting networks and reveals the cutting edge of irregular warfare. The complex

[835] U.S. Joint Forces Command, "Cross Functional Fusion Cells: Application of Tactical Fusion Cells at Higher Echelons," Concept White Paper V 1.5 (January 8, 2008), 3.

[836] Lamb and Munsing, *Secret Weapon*, 23.

[837] Ibid., 29.

insurgency in Iraq formed the venue for this conflict, which provided a unique environment as well. The initial phase of the war against AQI, from 2003–2006, revealed an inexcusable lack of overall U.S. understanding of the environment and the threat. Despite basic COIN doctrine and the notable examples of a few units "getting it right," most of the U.S. and coalition forces applied concepts were based primarily on traditional forms of warfare. These largely conventional approaches were ill-suited to a complex irregular war set in a culturally diverse and fragmented society. As a result, the United States sought to transition responsibility quickly to Iraqi forces, maintain a force protection posture, and was determined to stay out of the internal fight. AQI's strategy of devastating attacks succeeded in starting a sectarian civil war, and brought the country to the brink of collapse, but its coercive attempts at maintaining control in Al-Anbar backfired and resulted in the loss of much of its Sunni support base. In effect, AQI's overall strategy fragmented the very social networks it relied upon to build a cohesive resistance.

During the second phase of the conflict, from late 2006–present, U.S. efforts changed dramatically and the Sunni tribal leadership rejected AQI's violent dominance. This rejection allowed for the building of popular-based U.S. support networks, composed of tribal leadership and their militias. A comprehensive strategy and a new commander who emphasized its application provided strategic unity and direction for U.S. forces. At the same time, violence in Iraq was at epic proportions and people were willing to embrace the security provided by U.S. forces. In addition to providing local security, the strategic emphasis translated into tactical innovations as small units began to adapt to understanding the environment and interact with the population to a greater degree. These small units, many at the platoon level, formed numerous outposts throughout contested areas, ensuring 24/7 security and empowering local Iraqi security efforts. Overall, organizational integration between conventional, SOF, and inter-agency elements provided a high degree of collaboration, which developed the capability to execute effective strategy. This strategy maximized the utility of each element involved in the fight and allowed for a "squeeze" against irreconcilables at the fringes, which provided them with the existential decision to support local security efforts or be targeted.

U.S. Counter-Network Performance				
	Offensive Swarming	Illumination	Information Disruption	Fusion
1st Phase of Iraq Insurgency	-	+	-	-
2nd Phase of Iraq Insurgency	+++	+++	++	+++

Table 13. Overall U.S. Performance against AQI Fighting Network[838]

The U.S. effort against AQI provides clear indications of a successful counter-network framework, one that developed through experience gained in a complex irregular war. The threat posed by AQI revealed itself in horrific attacks, launched not by a centrally, controlled hierarchical organization, but by cells acting in a decentralized manner. Despite the overwhelming traditional superiority of the U.S. military, combating this threat required a strategy that integrated multiple entities, most notably the Sunni tribes and insurgents who rejected AQI. The application of this new strategy demonstrated a willingness to change and negated the threat in multiple ways through the effective application of counter-network variables.

The U.S.-led JSOTFs provided a high degree of offensive swarming, which complemented similar operations designed to control contested terrain, most notably in critical urban areas, such as Ramadi and Baghdad. An overwhelming operational tempo led to an increased amount of knowledge about AQI that provided benefits that led to further targeting and greater fidelity about the network itself. The latter facilitated greater pulsing to allow for patient collection against more significant segments and clusters within the network. At the tactical level, 24/7 raids, coupled with U.S. and Iraqi force partnership through contested areas, continually surprised AQI, which forced it onto the strategic defensive, shifted further north and become more isolated.

[838] This table provides a general depiction of the U.S. counter-network efforts and reveals the dramatic transformation of effort, which resulted in a successful counter-network performance. While some efforts began earlier than 2006, their effects became increasingly evident from 2006 onward.

In stark contrast to earlier U.S. efforts, improvements in illumination activities allowed for greater insight into AQI and the overall insurgency. The most telling aspect of illumination was a greater focus on social ties, insight gained through an increased understanding of the overall insurgency, and U.S. forces that doggedly connected with the local Iraqi population. Focusing such overall information was the increasing efficiency of exploitation activities, which meshed with multiple intelligence forms to provide the most valuable form of understanding the inner-workings of AQI's network. Exploitation both facilitated and benefitted from advances in infiltration and generated a combined level of HUMINT that became increasingly important, as AQI's pressured status that forced it to become even more clandestine in nature. Rapid advances and a dramatic increase in ISR led to the ability to focus quickly on operational activity, which contributed to the combined illumination gains.

Information disruption also provided significant gains, and its synchronization with operational activities formed a key element of U.S. information strategy. Consistent efforts at negating AQI's overall narrative were reinforced by its continued and overplayed application of horrific violence. Even the sectarian clash it provoked ultimately contributed more to its disruption and weakening than inciting Sunni backing. The successes displayed by U.S. information strategy were largely a result of AQI's information failures. U.S. collection and denial activities, more clearly focused, became increasingly effective as both technological and HUMINT capabilities developed in a synchronized manner. While time will tell how much deception was actually employed during the conflict, it most likely increased along with other information disruption efforts.

Providing an organizational and doctrinal basis for the combined interaction of the other counter-network variables, the U.S. application of fusion provides the clearest example of effectiveness. Organizationally, early fusion efforts were a tactical adaptation by innovative commanders and units that agreed to combine efforts against common problems. These efforts were then understood and capitalized on throughout the force and became more relevant under a common strategy of aggressively providing security and protecting the population. By incorporating each operating unit and supporting agencies,

fusion cells throughout Iraq provided the forum for a common understanding of the enemy, which led to a greater degree of fidelity and operational capability. The increasing incorporation of Iraqi intelligence and security forces into these efforts only enhanced their overall effects.

Overall, the U.S. and AQI conflict in Iraq provides perhaps the most balanced example of network-style warfare, which demonstrates the capabilities of a robust fighting network, but also a sophisticated counter-network response. A primary factor in this outcome was the synchronized effect of SOF, inter-agency and conventional units that showed a remarkable degree of collaboration against a fighting network. Further, the support of the tribal networks proved crucial to the overall pressure exerted against AQI. The initial phase of the conflict revealed, once again, the tremendous disparity between a modern military's capability and performance in an irregular warfare environment. However, the dramatic changes and experienced-based adaptation of the U.S. effort resulted in a remarkable turnaround that marked a second phase in which AQI lost the initiative. This loss of initiative resulted in its relentless pursuit and increasingly isolated position in Iraq.

VII. CONCLUSION

The dramatic changes of the information age affect modes of conflict as well, and even war is becoming "networked on an international scale."[839] Most attempts to describe the changes occurring in irregular warfare, whether military doctrine or academic literature, remain fixed on traditional modes of thought and corresponding definitions. While these schemas are not entirely invalid, as a whole they fail to address the nature of warfare in the information age, and in particular, the increasing empowerment of fighting networks. This study provides insight by applying a network perspective to irregular warfare and drawing this perspective beyond a conceptual level to a framework for countering such networks. This effort rejects basic attempts to reify networks, but instead utilizes the principles of the network perspective to demonstrate the dynamic nature of fighting networks, and the complexities of countering them.[840] Does it take a network to defeat a network? The simple answer is yes, but the full answer transcends organizational forms, which reveals war-fighting combinations that are truly unique.

A network is commonly thought of in strictly organizational terms, but the information age and the corresponding dynamics of globalization empower these organizational forms. In like manner, the fighting networks that increasingly dominate irregular warfare employ networked forms of organization, but they are just the fundamental building block for empowering other elements of war-fighting capacity. These irregular opponents form in networked configurations, which facilitate innovative doctrines, operational methods, and the use of information strategy to thrive in the information age as fighting networks. The organizational capacity of these networks is well-suited to benefit from the rapid advances of modern technology, but still retain the ability to do without, which demonstrates their remarkable flexibility.

---

[839] Hammes, *The Sling And the Stone*, 42.

[840] Kilcullen, "'Build It And They Will Come,'" 278.

The ability to acquire, utilize, and create meaningful information is at the core of the changing nature of irregular warfare. This essential nature focuses on basic questions of what, where, when, and why concerning one's opponents, and understands that the answers may be difficult to reach. In many ways, the changes in the information age favor the weaker opponent, by placing more value on the ability to shape information, than on the ability to employ forces or weapons. Given the premium on information, it is evident that the nature of irregular conflict is ambiguous and fluid, with hard-won information usually limited, fairly ambiguous, and often time sensitive.

Fighting networks thrive in such an environment, as their organizational design provides unique advantages for acquiring, processing, and most importantly, redistributing information. These organizational, doctrinal, and technological aspects of networks provide levels of functionality centered on the use of information. These systematic processes form much of their relevance and how they fight, and require a new way of looking at such threats. Prior descriptions, such as guerrillas, terrorists, and even insurgents, only capture a portion of what may be attributes of a fighting network. Useful in distinguishing various attributes of irregular networks, such as in describing tactics, or focusing on the political nature of a struggle, they are increasingly less relevant in capturing the changing nature of irregular warfare. In fact, modern fighting networks often blend these forms of warfare in ways that maximize their most positive attributes, which then produces hybrid forms whose flexibility is difficult to match.

Throughout this study, the use of network-style warfare, or netwar, provides a perspective that synthesizes many of these characteristics. While the netwar concept was originally framed to capture aspects of social conflict of a less violent nature, the rogue networks present in irregular warfare generate exceedingly violent versions. Network-style warfare defines much of current conflict, and while its proponents draw on other aspects of warfare, from the purely guerrilla to the conventional, this form of warfare is unique. Figure 17 illustrates the normal continuum, or spectrum of warfare, which is usually marked by low-intensity actions on one end, and high-intensity actions on the other. Netwar displays multiple characteristics, providing a unique form that challenges traditional ideas of a simple spectrum of conflict.

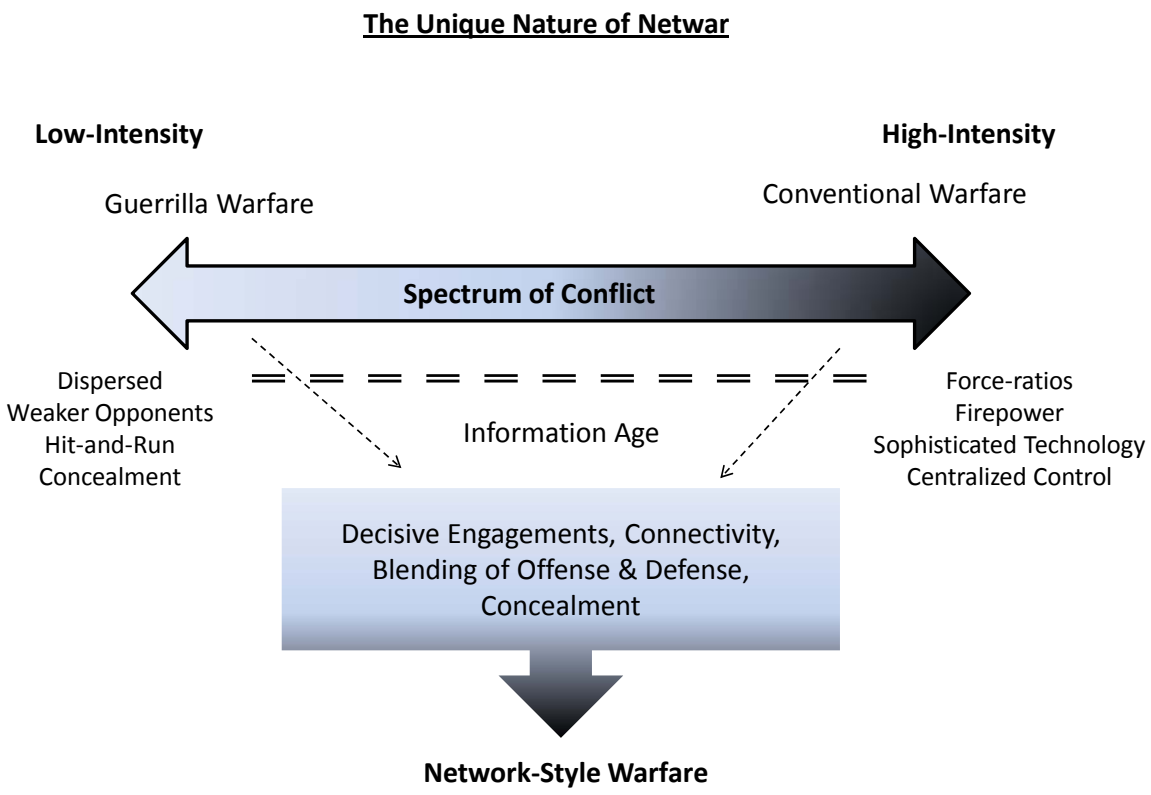

Figure 17. An Information Age Form of Conflict.

A. HOW NETWORKS FIGHT

Fighting networks display similarities to irregular combatants throughout the ages, with the distinguishing exception that they are not limited to just basic unconventional tactics, or guerrilla warfare. Instead, their form provides the means to utilize multiple styles of warfare, and provide the capability for a new range of doctrine and operational functions, which exploits the possibility that "the fundamental dynamic in future wars will more likely be that of 'hiders and finders,' with opposing forces surfacing only long enough to strike, then disappear."[841] Hezbollah provides a telling example of this blending of fighting styles and doctrine, so much so that it has generated

[841] Arquilla, *Worst Enemy*, 27.

significant debate about whether it is more conventional or guerrilla-like in nature. However, the diversity they display is not something that falls on a spectrum between guerrilla and conventional warfare, but is something entirely different.[842] Other information age networks reveal the same attributes, as Bruce Hoffman noted,

> It is possible then, that the insurgency in Iraq may perhaps represent a new form of warfare for a new, networked century. It is too soon to determine whether this development, involving loose networks of combatants who come together for discrete purpose only to quickly disperse upon its achievement will prove to be a lasting or completely ephemeral characteristic of postmodern insurgency. However, if it gains traction and is indeed revealed to be a harbinger of the future, the implications for how military forces train, equip, and organize to meet this challenge and avoid preparing to fight yesterday's—mostly, conventional—wars, will be of paramount importance.[843]

Further, due to their decentralized and generally distributed nature, networks are more readily able to take advantage of the increasing opportunities provided by modern information technology. This technology provides the means to further connectivity in ways unobtainable by irregular combatants of just 50 years ago. Yet, technology is just part of the story, which enhances what in many ways are more important organizational and doctrinal attributes. Perhaps most telling, the most advanced networks are those that arise from strongly connected societies that feature dense relational structures, such as clans and tribes. These traditional groupings provide unique bonds and levels of connection not readily obtained in today's modern nations, in which even the most professional militaries continue to strive for such levels of comradeship. The Chechen networks provide telling examples of these characteristics and their enhancement of warfighting ability.

However, networks have significant strengths and weaknesses, both of which provide aspects contributing to potential vulnerabilities. These strengths and weaknesses reside primarily in their organizational attributes, necessity for concealment, and information requirements. Understanding these strengths and weaknesses is crucial for

---

[842] Biddle and Friedman, *The 2006 Lebanon Campaign and the Future of Warfare*, 24, 73.

[843] Hoffman, "Insurgency and Counterinsurgency in Iraq," 115–116.

interaction with networks of any type and function, but especially critical when seeking to counter their violent actions. Networks cannot be fought using traditional methods, and the application of normal military force highlights their resiliency, adaptability, and concealment skills. However, understanding the informal, human connections that form networks provides the means to counter effectively, and even dramatically disrupt their efforts.

B. COUNTER-NETWORK THEORY

The identification of vulnerabilities provided the structural foundation for hypotheses leading to ways in which to counter networks. These hypotheses are directed at the question—how to fight networks? The recognition of shared characteristics between each hypothesis generated key variables for countering networks. At the core of these variables, and specific to their interaction, is the usage of information. However, recognizing the centrality of information does not mean that efforts must be directed to generate "information dominance," or that information technologies will provide a clear understanding of the battlefield for omniscient, centralized control. Ambiguity is a central aspect of war, as seen in the recent conflicts in Iraq and Afghanistan where "…enemy forces employed traditional countermeasures to coalition technological capabilities—measures such as dispersion, concealment, deception and intermingling with the civilian population."[844] Rather, understanding the importance of information leads to new doctrine, and operational methods, which maximize its role. The counter-network framework proposed in this study recognizes that a high level of ambiguity will always exist in irregular warfare, but that key variables contribute to a systematic approach to operations within such an environment.

These variables are fusion, illumination, offensive swarming, and information disruption, which provide the basic elements for countering fighting networks. Each of them addresses certain hypotheses-derived requirements for countering networks, and their combined nature provides a comprehensive approach to tackling and effectively

[844] H. R. McMaster, "On War: Lessons to be Learned," *Survival: Global Politics and Strategy* 50, no. 1 (2008): 21, http://dx.doi.org/10.1080/00396330801899439.

conducting operations against these tough opponents. Their common characteristic is information, which provides both requirements and the important synthesis of multiple activities. Each variable either provides ways to gain, process, or redistribute information, as well as disrupt an opponent by countering and denying their use of information, or using it to expose their activities.

Fusion addresses the requirement for a high level of connectivity within an organization. This connectivity promotes shared expertise and collaboration, which are essential qualities for understanding the complexity and cultural context of social networks, as well as forming the initial capacity to be as "agile" as networks. In addition, fusion requires a doctrinal component based on the unique requirements of irregular warfare, which recognizes the overwhelming importance of information, and combines operational and intelligence efforts to gain and understand information. Fusion provides the essential component upon which the other variables interact.

Illumination describes the process of understanding and identifying the key attributes and actions of fighting networks. Further, it begins with an effort to understand the social and cultural aspects of the human terrain in which networks form. This understanding recognizes that fighting networks are inherently different from traditional military opponents, and that traditional intelligence methods are insufficient for collection and analysis against them. Illumination covers the range of activities required to understand fighting networks and builds on the fusion of operations and intelligence to gain a greater understanding of networks than simply traditional intelligence methods.

Offensive swarming provides a doctrinal element, which is only possible through high levels of information and decentralized action. This capability stems from organizational fusion and the illumination efforts necessary to acquire and understand information about networked targets. The offensive nature of this swarming stems from the requirement to pressure clandestine fighting networks; thereby, depriving them of the initiative they gain from concealed, patient plotting. By retaining the offensive, swarming denies an enemy's requirement for surprise, and ensures that counter-network efforts retain the initiative.

Information disruption works in conjunction with kinetic offensive swarming, and should be applied in the same manner. Information disruption focuses specifically on addressing an opponent's information strategy, through collection, denial, and disruption of such efforts. The fundamental aspect of information disruption is countering or negating a fighting network's primary narrative, and nearly every other effort should support this strategy. Information disruption is also a synchronized effort, benefitting from, and generating, swarming and illumination. Recognizing the importance of information in irregular conflict, a strategy whose primary emphasis and majority of efforts are focused on information disruption, is most likely to succeed over any other approach.

C. CASE STUDY COMPARISON AND ANALYSIS

The cases examined in this study are each notable in their own right and highlight numerous irregular warfare truths. In addition, they each reflect the toughest irregular opponents of the emerging information age and feature fighting networks that have successfully countered much "superior" nation states. The examination of each case reinforced the basic fundamentals about how networks form, organize, and fight. Moreover, they reinforced the importance of strong social networks; fighting networks with such strong connections maintained a higher degree of effectiveness, while those who lost or failed to create such expanded structures, floundered. Each case expanded further upon the range of tactics and techniques employed by fighting networks, and demonstrated the remarkable innovation and change in irregular warfare, developments, which were diffused between the fighting networks in these case studies.

1. Russo-Chechen Case Study

The Russo-Chechen study revealed the inherent failure of traditional, largely conventional military attempts to counter a robust fighting network, but later reflects some degree of improvement. The 1st Russo-Chechen War resulted in a significant defeat for the Russians, which is the clearest such example among each of the clashes featured in this study. As a result, Russian efforts during their second invasion demonstrated some

degree of change, but this change was largely focused on repression of the Chechen fighting networks and their social foundations. Contributing factors, which display some aspects of the counter-network framework, were increased efforts to co-opt and partner with Chechens, greater illumination capabilities, and an information strategy that almost completely denied Chechen media access. Despite only displaying minimal counter-network characteristics, the Russians achieved a degree of success against Chechen fighting networks. However, this success was largely based on a strategy for control that is anathema to most modern Western militaries, and would most likely be far more effective, and longer lasting, in a counter-network framework. Overall, this case study demonstrated a slight degree of counter-network application and proportionate results.

2. Israel-Hezbollah Case Study

The Israel-Hezbollah case also featured a nearly entirely conventional attempt to fight a capable network, and with nearly no demonstration of counter-network capability. Israel's conflict with Hezbollah began in the early 1980s, and its evolution provided insight into the overall changes occurring in irregular warfare, as well as the increasing sophistication displayed by fighting networks. In the first conflict, initiated by the invasion in 1982, Israel's traditional efforts to maintain a buffer zone in southern Lebanon were increasingly undermined in the face of increased guerrilla activity. This conflict demonstrated Hezbollah's ability to build strong social networks, while developing the capability to transition from guerrilla tactics to more networked forms of military action. Hezbolllah's increasing ability for surprise swarming against Israeli outposts led to a growing loss of Israeli popular support and the eventual withdrawal of Israeli forces in 2000. In the 2006 campaign, Hezbollah demonstrated that fighting networks are increasingly able to confront, and defeat modern, professional militaries. A combination of factors, to include poor strategy, lack of training, and a fundamental misunderstanding of the enemy, led to Israel's poor performance. Hezbollah's remarkable defense demonstrated its unique blend of military doctrine and operational capability, and perhaps most significantly, the ability to dominate the information environment. Overall,

Israel demonstrated a near complete lack of counter-network understanding and capability. Israel's minor degree of offensive swarming was its initial aerial attacks against Hezbollah's missiles.[845]

3. U.S. vs. AQI Case Study

The U.S. conflict with AQI during the Iraqi insurgency provides another remarkable contrast between a superior military force and a highly networked opponent. The U.S. invasion of Iraq in 2003 demonstrated the combined war-fighting capabilities of a highly advanced military, but it was increasingly frustrated by the networked nature and sophisticated attacks launched by AQI. During the initial phase of the war, U.S. forces transitioned into an "overwatch" posture as political discussions and military strategy focused on withdrawal. AQI demonstrated success with its ability to inflict casualties and incite a sectarian conflict that nearly ripped Iraq apart. However, in the second phase of the insurgency, the United States changed its strategy and demonstrated remarkable capabilities for countering networked opponents. The second phase of the Iraqi insurgency provides the most complete application of the counter-network framework, and demonstrates the clearest example of success against a fighting network.

[845] Israel's more recent actions against Hamas in Gaza demonstrate a much higher level of success, which demonstrate increased capability following the 2006 conflict and reflect increased counter-network capabilities.

Overall Counter-Network Performance				
	Offensive Swarming	Illumination	Information Disruption	Fusion
1st Russo-Chechen War	-	-	-	-
2nd Russo-Chechen War	-	+	++	+
1st Israeli-Hezbollah War	-	-	-	-
2nd Israeli-Hezbollah War	+	-	-	-
1st Phase of Iraq Insurgency	-	+	-	-
2nd Phase of Iraq Insurgency	+++	+++	++	+++

Table 14. Cross-Case Comparison of Counter-Network Performance

Comparisons across the cases reveal the remarkable ability of fighting networks to persist against far superior professional militaries. As a test of the counter-network framework, each case study provides examples of a confrontation between a modern, professional military and a networked opponent. In two of the cases, some application of the counter-network variables occurred, which resulted in demonstrated successes. Repressive actions that resulted in some success in the Russo-Chechen conflict run counter to both the ethical restrictions governing most professional Western responses and the dynamics of information age conflict. Due to these imperatives, they were not used to modify the counter-network framework. Overall, the U.S. strategy and counter-network actions against AQI provide the most comprehensive example of the counter-network framework, and demonstrate remarkable success through its application. A look at the "results" demonstrates the following outcomes, in which success is a "win" with the opponent generally achieved its primary goals.

- 4 x "Win" for fighting network vs. traditional (Chechen, Hezbollah, and AQI)
- 2 x "Win" for counter-network vs. fighting network (Russian and U.S.)

- 4 x “Loss” for traditional v. fighting network (Russian, U.S., and Israel)
- 2 x “Loss” for fighting network vs. counter-network (Chechen and AQI)

Overall, these results demonstrate the ability of fighting networks to, at the least, deny their opponents their objectives, especially if those opponents are fighting in a traditional manner. In each portion of the study, networked forces succeeded against their opponents. The lack of success demonstrated by even the most sophisticated, technologically advanced militaries against fighting networks provides counter-factual suggestion in favor of a more networked approach. Likewise, the application of the counter-network framework generated success in two case studies, which provides evidence that reinforces the proposition that it takes a network to defeat a network. The U.S.-AQI case study provided a clear example of a highly networked professional force successfully demonstrating a counter-network approach and defeating a fighting network.

D. HOW TO FIGHT NETWORKS

These early conflicts between modern militaries and fighting networks provide consistent evidence of the nature of changes occurring in irregular warfare. Primarily, the nature of such conflicts features a highly networked opponent able to deny a nation-state’s attempts at control. In most of the clashes examined in this study, the fighting network succeeded, which clearly demonstrates their growing capabilities. While it is only one case, the results from the successful application of a counter-network framework in the U.S.-AQI case study provide a significant example of success. Further, because it is the most recent case studied, it highlights the adaptation of some forces, and perhaps, a trend toward more effective counter-network operations.

It is clear that irregular warfare cannot be separated from its inherent psychological, cultural, and political aspects, and that any attempt to counter networks must keep this as a core. In addition, this basic truth goes to the heart of building counter-networks and the strategies they employ. As Hammes states, “Western forces have tried to substitute technology for human connections. This is a fundamental difference [with our enemy] that must be recognized in the West. Once recognized, it should result in major efforts to build similar human networks among allies and neutrals when we are

fighting a networked insurgent."[846] Understanding the context of irregular warfare is essential to creating effective efforts against fighting networks. This understanding provides the initial, and what should be the primary, focus on the human and social dimensions of such conflict, and leads to the creation of effective strategic goals.

However, the principles and strategic application of network-style warfare are not limited to success in countering rogue networks. Beyond fighting these irregular opponents, the capabilities generated by a modern professional military that adopted network-style warfare could prove formidable against any other conventional force. The stark evidence for this capability is the performance of fighting networks with far fewer advantages derived from training, technology, and secure communications.

Organizationally, an effective counter-network framework requires emulating the increased connectivity and lower-level autonomy displayed by networks. While this imposes challenges for hierarchical military bureaucracies, much of the challenge results from simply adopting a different mindset, one that seeks to further connections. As Zanini and Edwards state, "while militaries and governments will never be able to do away with their hierarchies entirely, there is nonetheless much room for them to develop more-robust organizational networks than they currently have—a change that may offset some, if not all, of the advantage now accruing to networked terrorist groups."[847] An increased emphasis on lateral communication and connections throughout a military organization would promote many of the same connections. Fostering such connections requires training and employing individuals in such a manner that they seek to build such ties, which leads to a robust informal network. Developing such organizational capability is about valuing expertise and experience more than position, and promoting connections for the increased power they provide for greater information acquisition and redistribution. These efforts should be complemented with an increased emphasis on training and rewarding those confident and capable of operating within a fluid, networked environment. In addition to internal connections, an effective counter-network

[846] Thomas X. Hammes, "Rethinking the Principles of War: The Future of Warfare," in *Rethinking the Principles of War*, ed. Anthony McIvor (Annapolis, MD: Naval Institute Press, 2005), 276.

[847] Zanini and Edwards, "The Networking of Terror in the Information Age," 55.

organization builds external connections, and is able to form rapid partnerships oriented towards a common purpose. This aspect requires additional effort, but it appears it is the most effective way to maximize the various skills and expertise required to counter networks. Further, networking externally provides the means to enhance opportunities and invigorate much of the bureaucratic inertia and restrictions within static organizations. It may be that more static hierarchies remain, but that they provide resources and efficient backing to further networks at the operational level.

The doctrinal challenge in countering networks is to develop principles and practices that seek to maximize the inherent superiorities of a professional military by combining them in ways better suited to effective information age organization. The primary challenge is the inherent levels of control in a machine-type bureaucracy, a requirement that drives doctrine requiring a high level of command and control. However, recent experience in irregular warfare reinforces the necessity of small-unit action, empowered lower-level commanders, and change driven by innovative operators. As seen in multiple examples of swarming, many of the doctrinal types well-suited for information-age conflict require both significant amounts of information and a great deal of decentralization. This decentralization is imperative for bottom-up innovation and fostering connections at the local, or lowest, levels. As seen in the Iraq case study, the application of a common strategy promoted doctrinal innovation and lower-level action by providing an overarching purpose. While a COIN focus provided the umbrella for multiple types of successful action, it may not prove to be the most effective doctrine for countering future irregular threats. Countering future irregular forces will most likely require indirect elements of COIN, but also elements of direct disruption, such as CT. Moreover, as the intensity of irregular warfare increases, it is likely to require the innovative blending of heavy weapons with precision application. These changes, and numerous others, will require new doctrinal aspects, which will most likely be generated by a new generation of network-focused forces with combat-generated learning and innovation. In stark contrast to current efforts promoting NCW as a means to achieve

superior information and precisely control a combat environment, doctrine stemming from a netwar focus will recognize the chaos and complexity inherent in conflict, and generate increased levels of flexibility in spite of it.

Operationally, those seeking to counter fighting networks must realize the asymmetric nature of their enemy's tactics and the synthesis between tactical action and information effects. While fighting networks utilize many of the basic methods employed by irregular opponents throughout guerrilla warfare, they have also adapted and generated new methods for the information age. Actions, such as human-guided suicide attacks and systems disruption, reflect a blending of operational methods, tactics, and information designed to achieve greater effect. Cordesman provides a sense of this blending in his assessment of required operational changes:

> In optional and limited wars, Western nations must learn how to fight in built-up and populated areas in ways that do as much as possible to deprive the enemy of the ability to force modern military forces to fight at the enemy's level, as well as in asymmetric ways that deprive conventional forces of their technical advantages and give the enemy the initiative. This change not only involves altering tactics and targeting but also means funding suitable ISR assets; putting HUMINT in the loop; having dedicated cells to warn when given targets or when targeting data prevent special sensitivities; and using small, reliable, precision weapons wherever possible. It also means tailoring information operations to fight what will inevitably be a global battle to prove that targeting is valid and that every effort is being made to reduce civilian casualties and collateral damage.[848]

These changes are essential for countering networks, which rely on the fact that traditional asymmetries between professional militaries and irregular forces favor their flexible, adaptable nature. Operational methods must synchronize efforts that deny a network's concealment, to disrupt its use of surprise. This effort requires small units that are just as flexible, and which, turn the tables by utilizing the same aspects of concealment and rapid strikes to surprise and achieve the initiative. These small units achieve greater effectiveness by being connected and taking self-synchronized actions against a rapidly changing enemy network.

---

[848] Cordesman, *Lessons of the 2006 Israeli-Hezbollah War*, 49.

At its core, irregular warfare is about information, and a conflict between networks is truly a contest between information strategies. On the strategic level, effective counter-network efforts place the primary emphasis on disrupting a fighting network's overall narrative and information campaigns. For these efforts to be effective, they must both disrupt a network's external information flow, or public message, while at the same time, "claiming the space" with another message. This other message, or counter-narrative, must by consistent and synthesized with operational action to produce a compelling link between word and deed. As evidenced in AQI's excessive coercion producing the Al-Anbar Awakening, as well as the fallout from Abu Ghraib, information strategy without corresponding action is meaningless. Where clashes occur, the outcome usually favors the opponent with greater information, and those small units able to leverage the most information against their targets. In this regard, the targeting cycles employed by counter-network forces are examples of focused information collection and processing, applied most effectively to disrupt a fighting network's connections, and as a result, their ability to collect, process, and redistribute information.

In summary, the threat posed by fighting networks requires a concerted counter-network effort, which adapts to and innovates in the changing environment of the information age. Fighting networks present a unique challenge, one that reflects the timeless nature of irregular warfare, while simultaneously ushering in dramatic changes. Displaying a fairly remarkable "track-record" against the most sophisticated modern forces, these networks highlight the empowerment of unconventional forces and doctrine. The framework proposed and tested in this study provides an synthesized operational perspective to counter these fighting networks.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Abizaid, General John. Department of Defense briefing transcript. July 16, 2003. Cited in Anthony Cordesman, *The Iraq War: Strategy, Tactics, and Military Lessons*. Westport, CT: Praeger Publishers, 2003.

Abu Bakr Naji. "The Management of Savagery." In *The Canons of Jihad*, edited by Jim Lacey, 62. Annapolis, MD: Naval Institute Press, 2008.

Acosta, David A. "The Makara of Hezbollah: Deception in the 2006 Summer War." Master's thesis, Monterey, CA: Naval Postgraduate School, 2007.

Adams, Barbara D., and Robert D. G. Webb. "Trust in Small Military Teams." Accessed March 19, 2011. http://www.dodccrp.org/events/7th_ICCRTS/Tracks/pdf/006.PDF.

al-Alwani, Governor Mamoun Sami Rashid. Quoted in Gary W. Montgomery and Timothy S. McWilliams, *Al-Anbar Awakening, Volume II: Iraqi Perspectives, From Insurgency to Counterinsurgency in Iraq, 2004–2009*, 155. Washington, DC: Government Printing Office, 2009.

Al-Anbar Awakening, Volume II: Iraqi Perspectives, From Insurgency to Counterinsurgency in Iraq, 2004–2009. Washington, DC: Government Printing Office, 2009)

al-Assafi, Sheikh Ali Hatim. Quoted in Gary W. Montgomery and Timothy S. McWilliams, *Al-Anbar Awakening, Volume II: Iraqi Perspectives, From Insurgency to Counterinsurgency in Iraq, 2004–2009*. Washington, DC: Government Printing Office, 2009.

al-Bassam, Maryam. "Interview with Hizbollah Leaer Hasan Nasrallah." *Beirut New TV Channel*, aired August 27, 2006. Quoted in Daniel Helmer, "Not Quite Counterinsurgency: A Cautionary Tale for the US Forces Based on Israel's Operation Change of Direction." *Armor* CXVI, no. 1 (January–February 2007). Accessed May 4, 2011. https://www.knox.army.mil/center/armormag/currentissues/2007/Jf07/1Helmer07c.pdf.

Al-Jabouri, Najim Abed, and Sterling Jensen. "The Iraqi and AQI Roles in the Sunni Awakening." *Prism* 2, no. 1 (2010).

al-Muqrin, Abd al-Aziz. *Al-Qa'ida's Doctrine for Insurgency: "A Practical Course for Guerrilla War" Translated and Analyzed by Norman Cigar*. Translated by Norman L. Cigar. Dulles, VA: Potomac Books, 2009.

al-Musawi, Ahmad. “Shahada wa-istishhadiyyin.” *Al-Shira’a*, June 5, 2000.

al-Suri, Abu Musab. “The Global Islamic Resistance Call.” In *Architect of Global Jihad: The Life of Al-Qaeda Strategist Abu Mus’ab al-Suri*, edited by Brynjar Lia. New York: Columbia University Press, 2008.

al-Zarqawi, Abu Mus’ab. May 11, 2004. Videotaped Broadcast, cited in Jean-Charles Brisard, *Zarqawi: The New Face of Al-Qaeda*. New York: Others Press, 2005.

Allawi, Ali A. *The Occupation of Iraq: Winning the War, Losing the Peace*. New Haven, CT: Yale University Press, 2007.

Arkin, William. *Divining Victory: Airpower in the 2006 Israel-Hezbollah War*. Maxwell AFB, AL: Air University Press, 2007.

Arquilla, John. “The End of War as We Knew It? Insurgency, Counterinsurgency and Lessons from the Forgotten History of Early Terror Networks.” *Third World Quarterly* 28, no. 2 (2007): 369–386.

———. “Thinking About Information Strategy.” In *Information Strategy and Warfare: A Guide to Theory and Practice,* edited by John Arquilla and Douglas A. Borer. New York: Routledge, 2007.

———. *Aspects of Netwar & the Conflict with Al-Qaeda*. Monterey, CA: Naval Postgraduate School, Information Operations Center, 2009.

———. *Worst Enemy: The Reluctant Transformation of the American Military*. Chicago: Ivan R. Dee, 2008.

Arquilla, John, and David F. Ronfeldt. *The Advent of Netwar*. Santa Monica, CA: RAND, 1996.

———. ed. *In Athena’s Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND, 1997.

———. “Networks, Netwars, and the Fight for the Future.” Accessed March 24, 2011. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/889/798.

———. The Advent of Netwar (Revisited).” In *Networks and Netwar*, edited by John Arquilla and David Ronfeldt, 19. Santa Monica, CA: RAND, 2001.

———. *Network and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND, 2001.

———. *Swarming and the Future of Conflict*. Santa Monica, CA: RAND, MR-1100-OSD, 2000.

Arquilla, John, and Douglas A. Borer. “Strategic Dimensions of the Iraq Conflict.” In *The Three Circles of War: Understanding the Dynamics of Conflict in Iraq*, *The Three Circles of War: Understanding the Dynamics of Conflict in Iraq*, edited by Heather S. Gregg, Hy S. Rothstein, and John Arquilla, 181. Washington, DC: Potomac Books, 2010.

Arquilla, John, and Theodore Karasik. “Chechnya: A Glimpse of Future Conflict?” *Studies in Conflict and Terrorism* 22, no. 3 (July–September 1999): 207–230.

Asprey, Robert B. *War in the Shadows: The Guerrilla in History*. New York: Doubleday & Company, Inc., 1975.

Baddeley, John. *The Russian Conquest of the Caucasus*. London: Longmans Green & Co., 1908.

Banks, William C., Renée de Nevers, and Mitchel B. Wallerstein. *Combating Terrorism: Strategies and Approaches*. Washington, DC: CQ Press, 2008.

Barabási, Albert-László, and Eric Bonabeau. “Scale Free Networks.” *Scientific America* 288, no. 5 (May 2003): 50–59. Accessed February 18, 2011. http://www.nd.edu/~networks/Publication%20Categories/01%20Review%20Articles/ScaleFree_Scientific%20Ameri%20288,%2060-69%20(2003).pdf.

Barabási, Albert-László, and Rika Albert. “Emergence of Scaling in Random Networks.” *Science* 286 (1999): 509–512.

Barabási, Albert-László. *Linked: The New Science of Networks*. Cambridge, MA: Perseus Books, 2002.

Barak, Ehud. *Newsweek*, July 18, 2006.

Baram, Amatzia, “Neo-Tribalism in Iraq: Saddam Hussein’s Tribal Policies 1991–96.” *International Journal of Middle East Studies* 29, no. 1 (1997): 1–31. Accessed May 15, 2011. http://www.jstor.org/stable/163849.

Bar-Joseph, Uri. “Israel’s Military Intelligence Performance in the Second Lebanon War.” In *International Journal of Intelligence and Counterintelligence* 20, no. 4 (2007): 583–601. Accessed May 7, 2011. http://dx.doi.org/10.1080/08850600701472970.

Bell, J. Bowyer. “Aspects of the Dragonworld: Covert Communication and the Rebel Ecosystem.” *International Journal of Intelligence and Counterintelligence* 3, no. 1 (1989): 15–43.

———. “Revolutionary Dynamics: The Inherent Inefficiency of the Underground.” *Terrorism and Political Violence* 2, no. 2 (Summer 1990): 193–211.

Bennett, Brian. “On Scene: How Operation Swarmer Fizzled.” *Time*, March 17, 2006. Accessed May 15, 2011. http://www.time.com/time/world/article/0,8599,1174448,00.html.

Bergen, Peter. “After the War in Iraq: What Will the Foreign Fighters Do?” In *Bombers, Bank Accounts, and Bleedout*, edited by Brian Fishman, 109. West Point, NY: Combating Terrorism Center, 2007.

———. *The Longest War: The Enduring Conflict Between America and Al-Qaeda*. New York: Free Press, 2011.

Berger, Ronald L. “The Analysis of Social Networks.” In *Handbook of Data Analysis*, edited by Melissa Hardy and Alan Byman, 505–526. London: SAGE Publications, 2004.

Bergman, Ronen. *The Secret War with Iran*. New York: Simon & Schuster, 2008.

Berkowitz, Bruce, *The New Face of War: How War Will be Fought in the 21st Century*. New York: The Free Press, 2003.

Bianconi, Ginestra, and Albert-László Barabási. “Competition and Multi-scaling in Evolving Networks, “*Europhysics Letters (EPL)* (2001): 436–442.

Biddle, Stephen, and Jeffrey A. Friedman. *The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy*. Carlisle, PA: U.S. Army War College Strategic Studies Institute, 2008.

Biddle, Stephen. “Land Warfare: Theory and Practice.” In *Strategy in the Contemporary World: An Introduction to Strategic Studies*, edited by James Wirtz, Eliot Cohen and John Baylis. Oxford, UK: Oxford University Press, 2002.

bin Laden, Osama. Quoted in “Osama Bin Laden to the Iraqi People.” MEMRI Special Dispatch no. 837, *Middle East Research Institute*. Accessed March 9, 2011. http://www.memri.org/report/en/0/0/0/0/0/0/1286.htm.

Blandy, Charles W. *Chechnya: Dynamics of War Brutality and Stress*. Sandhurst, UK: The Conflict Studies Research Center, 2001. Accessed March 16, 2011. www.da.mod.uk/colleges/arag/document-listings/caucasus/P35.

———. *Chechnya: Two Federal Interventions: An Interim Comparison and Assessment*. Sandhurst, UK: The Conflict Studies Research Center, 2000. Accessed March 16, 2011. www.da.mod.uk/colleges/arag/document-listings/caucasus/P29.

———. *North Caucasus: Negative Trends*. Shrivenham, UK: Defence Academy of the UK, 2009. Accessed May 23, 2011. www.da.mod.uk/colleges/arag/document-listings/caucasus/09%2812%29%20CWB%203.pdf.

Blanford, Nicholas. “Hizbullah and the IDF: Accepting New Realities Along the Blue Line.” In *The Sixth War: Israel’s Invasion of Lebanon, The MIT Journal of Middle East Studies* 6 (Summer 2006). Accessed April 20, 2011. http://web.mit.edu/cis/www/mitejmes/.

Blank, Stephen J., and Earl H. Tilford. *Russia’s Invasion of Chechnya: A Preliminary Assessment*. Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 1995.

Bodansky, Yossef. *The Secret History of the Iraq War*. New York: Harper and Collins, 2004.

Bolman, Lee G., and Terrence E. Deal. *Modern Approaches to Understanding and Managing Organizations*. San Francisco, CA: Jossey-Bass, 1984.

Boon, Susan D., and John G. Holmes. “The Dynamics of Interpersonal Trust: Resolving Uncertainty in the Face of Risk.” In *Cooperation and Prosocial Behavior*, edited by Robert Hindle and Jo Groebel, 167–182. New York: Cambridge University Press, 1991. Cited in Barbara D. Adams and Robert D. G. Webb, “Trust in Small Military Teams.” Accessed April 14, 2011. http://www.dodccrp.org/events/7th_ICCRTS/Tracks/pdf/006.PDF.

Boyle, Michael J. “Do Counterterrorism and Counterinsurgency Go Together?” *International Affairs* 86, no. 2 (2010): 333–353, Blackwell Publishing, Ltd.

Brisard, Jean-Charles. *Zarqawi: The New Face of Al-Qaeda*. New York: Others Press, 2005.

Buchanan, Mark. *Nexus: Small Worlds and the Groundbreaking Theory of Networks*. New York: W.W. Norton & Company, Inc., 2003.

Burki, Shireen K. “Ceding the Ideological Battlefield to Al-Qaeda: The Absence of an Effective U.S. Information Strategy.” In *Comparative Strategy* 28, no. 4 (September 2009): 349–366. Accessed May 18, 2011. http://dx.doi.org/10.1080/01495930903185351.

Bush, George W. *The National Strategy for Combating Terrorism*. Washington, DC: The White House, February, 2003.

Byman, Daniel. “Understanding Proto-Insurgencies.” *Journal of Strategic Studies* 31, no. 2 (2008): 165–200. Accessed May 1, 2011. http://dx.doi.org/10.1080/01402390801940310.

Callwell, Charles E. *Small Wars: A Tactical Textbook for Imperial Soldiers* (1906). Novato, CA: Presidio Press, 1990.

Caraccilo, COL Dominic J., and LTC Andrea L. Thompson. *Achieving Victory in Iraq: Countering an Insurgency*. Mechanicsburg, PA: Stackpole Books, 2008.

Carley, Kathleen M., Ju-Sung Lee, and David Krackhardt. "Destabilizing Networks." *Connections* 24, no. 3 (2002): 79–92.

Carter, David L. "The Intelligence Fusion Process." *Intelligence*, 2008.

Carter, David L., and Jeremy G. Carter. "The Intelligence Fusion Process for State, Local, and Tribal Law Enforcement." *Criminal Justice and Behavior* 36, no. 12 (2009).

Cassidy, Robert M. *Russia in Afghanistan and Chechnya: Military Strategic Culture and the Paradoxes of Asymmetric Conflict*. Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 2003. Accessed April 4, 2011. http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB125.pdf.

Castells, Manuel. *The Rise of the Network Society*. Cambridge, MA: Blackwell, 1996.

Cave, Damien, and James Glanz. "Toll in Iraq Bombing is Raised to More Than 500." *New York Times*, August 22, 2007.

Cebrowski, Vice Admiral Arthur, and John Garstka. "Network-Centric Warfare." *Proceedings of the Naval Institute* 124, no. 1 (1998): 28–35.

Chaliand, Gerard, ed. *Guerrilla Strategies: An Historical Anthology from the Long March to Afghanistan*. Berkeley: University of California Press, 1982.

"Chechen Rebel Says He Ordered Moscow Metro Attacks." *BBC News*, March 31, 2010. Accessed April 11, 2011. http://news.bbc.co.uk/2/hi/8597792.stm.

Chernomorskiy, Pavel. "Second Chechen War on the Internet: Total Defeat?" (in Russian), *Internet.ru*, February 18, 2000. Accessed April 26, 2011. http://www.internet.ru/preview_a/articles/2000/02/18/1760.htm. Cited by Olga Oliker, *Russia's Chechen Wars 1994–2000: Lessons Learned from Urban Combat*. Santa Monica, CA: RAND, 2001.

Christakis, Nicholas A., and James H. Fowler. *Connected*. New York: Little Brown and Company, 2011.

Clausewitz, Carl Von. *On War*. Edited by and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1989.

Cline, Lawrence E. *Pseudo Operations and Counterinsurgency Lessons from Other Countries*, United States Army War College Strategic Studies Institute, June 2005. Accessed March 8, 2011. http://www.carlisle.army.mil/pubs/display.cfm?pubID=607.

Cobban, Helena. *The Making of Modern Lebanon*. Boulder, CO: Westview Press, 1985.

Cody, Edward, and Molly Moore. "'The Best Guerrilla Force in the World:' Analysts Attribute Hizballah's Resilience to Zeal, Secrecy and Iranian Funding." *The Washington Post*, A.1, August 14, 2006. Accessed April 22, 2011. http://search.proquest.com.libproxy.nps.edu/docview/410019829/12F16F8BD2A754B8925/1?accountid=12702.

Collins, Joseph. "An Open Letter to President Bush." *Armed Forces Journal* (January 2006). Accessed May 24, 2011. http://www.armedforcesjournal.com/2006/01/1403023/.

"The Commission for the Investigation of the Battle in Lebanon in 2006, the Second Lebanon War." *The Winograd Commission Report*, An Interim Report, April 30, 2007. Accessed April 28, 2011. http://www.cfr.org/israel/winograd-commission-partial-report/p13228.

"Confession of Umar Bazyani to Iraqi Security Forces." Accessed March 12, 2011. http://www.redorbit.com/news/international/415538/copy_of_security_report_on_alzraqawi_ansar_alsunnah_groups_/index.html.

Conway, Gen. James T., Adm Gary Roughead, and Adm Thad W. Allen. *A Cooperative Strategy for Maritime Security*. Washington, DC: Department of the Navy, 2007.

Coram, Robert. *Boyd: The Fighter Pilot Who Changed the Art of War*. New York: Back Bay Books, 2004.

Cordesman, Anthony. *Lessons of the 2006 Israeli-Hezbollah War*. Washington, DC: Center for Strategic and International Studies Press, 2007.

Crenshaw, Martha. "How Terrorism Declines." *Terrorism and Political Violence* 3, no. 1 (1991): 47.

———. "The Logic of Terrorism: Terrorist Behavior as a Product of Strategic Choice." In *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, edited by Walter Reich, 20–21. London: Cambridge University Press, 1990.

Creveld, Martin van. *The Changing Face of War*. New York: Ballantine Books, 2006.

———. *The Transformation of War*. New York: The Free Press, 1991.

Cronin, Audrey Kurth. "Behind the Curve: Globalization and International Terrorism." *International Security* 27, no. 3 (Winter 2002/2003): 30–58. Accessed February 28, 2011. http://www.jstor.org/stable/3092113.

Crooke, Alastair. and Mark Perry. “How Hezbollah Defeated Israel, Part 2: Winning the Ground War.” *Asia Times Online*, October 13, 2006. Accessed April 21, 2011. http://www.atimes.com/atimes/Middle_East/HJ13Ak01.html.

Davis, Eric. *Memories of State: Politics, History, and Collective Identity in Modern Iraq*. Berkley, CA: University of California Press, 1978.

Davis, Ian S., Carrie L. Worth, and Douglas Zimmerman. “A Theory of Dark Network Design.” Master’s thesis, Monterey, CA: Naval Postgraduate School, 2010.

Davison, MAJ Ketti C. “Systemic Operational Design (SOD): Gaining and Maintaining the Cognitive Initiative.” Fort Leavenworth, KS: United States Army Command and General Staff College, 2006.

de Nooy, Wouter, Andrej Mrvar, and Vladimir Batagelj. *Exploratory Social Network Analysis with Pajek*. New York: Cambridge University Press, 2008.

Deeb, Lara. “Deconstructing a ‘Hizbullah Stronghold’.” In *The Sixth War: Israel’s Invasion of Lebanon*, *The MIT Journal of Middle East Studies* 6 (Summer 2006). Accessed April 20, 2011. http://web.mit.edu/cis/www/mitejmes/.

Dixon, Nancy M., Nate Allen, Tony Burgess, Pete Kilner, and Steve Schweitzer. *Company Command: Unleashing the Power of the Army Profession*. Center for the Advancement of Leader Development & Organizational Learning, 2005.

Doorey, CAPT Timothy J. “Waging an Effective Strategic Communications Campaign in the War on Terror.” In *Ideas As Weapons: Influence and Perception in Modern Warfare*, edited by G. J. David Jr. and T. R. McKeldin III, 145. Washington, DC: Potomac Books, 2009.

Dressler, Jeffrey A. *The Haqqani Network: From Pakistan to Afghanistan*. Washington, DC: Institute for the Study of War, 2010.

Duffield, Mark. “War as a Network Enterprise: The New Security Terrain and Its Implications.” *Cultural Values* 6, no. 1 (2002): 153–165. Accessed March 1, 2011. http://www.idrc.ca/uploads/user-S/10588048681Duffield_netwar2.pdf.

Dunlop, John B. *Russia Confronts Chechnya: Roots of a Separatist Conflict*. London: Cambridge University Press, 1998.

Dunnigan James, and Albert Nofi. “Deception Explained, Described, and Revealed.” *Victory and Deceit: Dirty Trick in War*. New York: William Morrow, 1995, referenced in David A. Acosta, “The Makara of Hezbollah: Deception in the 2006 Summer War.” Master’s thesis, Monterey, CA: Naval Postgraduate School, 2007.

Dupuy, Trevor N., and Paul Martell. *Flawed Victory: The Arab-Israeli Conflict and the 1982 War in Lebanon*. Fairfax, VA: Hero Books, 1986.

Eack, Kevin D. “State and Local Fusion Centers: Emerging Trends and Issues.” *Homeland Security Affairs*. Accessed March 19, 2011. http://www.hsaj.org/index.php?fullarticle=supplement.2.3.

Edwards, Sean J. A. *Swarming and the Future of Warfare*. Santa Monica, CA: RAND, 2005.

Eggen, Dan, and Scott Wilson. “Suicide Bombs Potent Tools of Terrorists.” *Washington Post*, July 17, 2005. Accessed May 17, 2011. http://www.washingtonpost.com/wp-dyn/content/article/2005/07/16/AR2005071601363.html.

Eilstrup-Sangiovanni, Mette, and Calvert Jones. “Assessing the Dangers of Illicit Networks: Why Al-Qaida May Be Less Threatening Than Many Think.” *International Security* 33, no. 2 (Fall 2008): 7–44.

Ellis, John. *A Short History of Guerrilla Warfare*. London, 1975.

Engel, Eloise, and Lauri Paananen. *The Winter War: The Soviet Attack on Finland 1939–1940*. Mechanicsburg, PA: Stackpole Books, 1973.

Erickson, Bonnie H. “Secret Societies and Social Structure.” *Social Forces* 60, no. 1 (1981): 188–210. Accessed November 15, 2010. http://www.jstor.org/stable/2577940.

Everton, Sean. *Tracking Destabilizing and Disrupting Dark Networks with Social Network Analysis*. Monterey, CA: Naval Postgraduate School, 2009.

Exum, Andrew. *Hizballah at War: A Military Assessment*, Policy Focus No. 63. Washington, DC: The Washington Institute for Near East Policy, 2006. Accessed April 28, 2011. 10. http://www.washingtoninstitute.org/pubPDFs/PolicyFocus63.pdf.

Falichev, Oleg. “FCS Will Certainly Publish Information on Who Helped Dudayev and How.” *Krasnaia avezda*, January 21, 1995, 2. Cited in John Arquilla and Theodore Karasik. “Chechnya: A Glimpse of Future Conflict?” *Studies in Conflict and Terrorism* 22, no. 3 (July–September 1999): 207–230.

Farrell, Stephen. “Around 150, Death Toll in Iraq Attack Among War’s Worst.” *New York Times*, July 9, 2007.

Fearon, James D. “Iraq’s Civil War.” *Foreign Affairs* 86, no. 2 (March–April, 2007): 2–15. Accessed May 19, 2011. http://www.jstor.org/stable/20032280.

Finch, MAJ Raymond C. “Why the Russian Military Failed in Chechnya.” *Foreign Military Studies Office Special Study 98–16*. Fort Leavenworth, KS: Center For Army Lessons Learned, 1998.

Finlan, Alastair. *Special Forces, Strategy and the War on Terror: Warfare by Other Means*. New York: Routledge, 2007.

Fishman, Brian, "After Zarqawi: The Dilemmas and Future of Al-Qaeda in Iraq." *The Washington Quarterly* 29, no. 4 (2006): 19–32. Accessed May 10, 2011. http://dx.doi.org/10.1162/wash.2006.29.4.19.

Fishman, Brian, and Joseph Felter. *Al-Qaida's Foreign Fighters in Iraq: A First Look at the Sinjar Records*. West Point, NY: Combating Terrorism Center, 2007.

Fishman, Brian, *Dysfunction and Decline: Lessons Learned from Al-Qaeda in Iraq*. West Point, NY: Combating Terrorism Center, 2009.

Flynn, Michael T., Matt Pottinger, and Paul D. Batchelor. *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*. Washington, DC: Center for a New American Security, 2010. Accessed May 21, 2011. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA511613&Location=U2&doc=GetTRDoc.pdf.

Flynn, Michael T., Rich Juergens, and Thomas L. Cantrell. "Employing ISR: SOF Best Practices." *Joint Forces Quarterly* 50 (3rd Quarter): 57. Accessed November 15, 2010. https://digitalndulibrary.ndu.edu/u?/ndupress,20540.

Fogarty, Brendan. "Chechnya Redux? Violent Conflict in Ingushetia." *Harvard International Review* 31, no. 4 (January 1, 2010): 8. Accessed November 14, 2010. http://www.proquest.com.libproxy.nps.edu/.

Freedman, Lawrence. *The Transformation of Strategic Affairs*. Abingdon, NY: Routledge, 2006.

Freier, Nathan. *Small Wars 2.0: A Working Paper on Land Force Planning After Iraq and Afghanistan*. Carlisle Barracks, PA: U.S. Army Peacekeeping and Stability Operations Institute, 2011. Accessed March 1, 2011. http://pksoi.army.mil/PKM/publications/relatedpubs/documents/Small_Wars_2.0.pdf.

"Full Text of Colin Powell's Speech: U.S. Secretary of State's Address to the United Nations Security Council." *The Guardian*. Accessed March 8, 2011. http://www.guardian.co.uk/world/2003/feb/05/iraq.usa.

Fussell, LCDR Christopher L., MAJ Trevor M. Hugh, and MAJ Matthew D. Pedersen. "What Makes Fusion Cells Effective?" Master's thesis, Monterey, CA: Naval Postgraduate School, 2009.

Galbraith, LTC Roger S. "Winning on the Information Battlefield: Is the Story Getting Out?" In *Ideas As Weapons: Influence and Perception in Modern Warfare*, edited by G. J. David Jr. and T. R. McKeldin III, 134. Washington, DC: Potomac Books, 2009.

Gall, Carlotta, and Thomas de Waal. *Chechnya: Calamity in the Caucasus*. New York: New York University Press, 1998.

Galula, David. *Counterinsurgency Warfare: Theory and Practice*, [1964]. Westport, CT: Praeger Security International, 2006.

———. *Counterinsurgency Warfare: Theory and Practice*. New York: Praeger Publishers, 1964).

Gann, Lewis H. *Guerrillas in History*. Stanford, CA: Hoover Institution Press, 1971.

George, Alexander L., and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press, 2005.

Gerges, Fawaz A. *Journey of the Jihadist: Inside Muslim Militancy*. Orlando, FL: Harcourt, 2006.

Gorka, Sebastian L. V., and David Kilcullen. "An Actor-Centric Theory of War: Understanding the Difference between COIN and Counterinsurgency." *Joint Forces Quarterly* 60, no. 1 (2011). National Defense University Press. Accessed February 8, 2011. http://www.ndupress.ndu.edu.

Graham, Thomas E. Jr. "Can Russia Win in Chechnya." *Brown Journal of World Affairs* 8, no. 1 (Winter/Spring 2001): 6.

Granovetter, Mark. "The Strength of Weak Ties." *American Journal of Sociology* (1973): 78, 1360–1380.

Grant, Greg. "The Man Behind Irregular Warfare Push: Mike Vickers." April 7, 2009. Accessed February 26, 2011. http://www.dodbuzz.com/2009/04/07/the-man-behind-irregular-warfare-push-mike-vickers.

Grau, Lester. "Changing Russian Urban Tactics: The Aftermath of the Battle of Grozny." First published in *INSS Strategic Forum* 38, July 1995. Accessed April 8, 2011. http://www.globalsecurity.org/military/library/report/1995/grozny.htm,

Greene, Thomas H. *Comparative Revolutionary Movements*. Englewood Cliffs, NJ: Prentice Hall, 1984.

Gudkov. Grennadii. Cited in Igor' Plugatarev, "Ukhod nachal'nika Genshtaba Kvashnina predopredelen: Kreml' gotovitsya nazvat' osnovnogo vinovnika za sluchivsheesya v Ingushetii." *Nezavisimoe voennoe obozrenie* no. 24, July 2, 2004, 1–2.

Gunaratana, Rohan, and Aviv Oreg. "Al-Qaeda's Organizational Structure and its Evolution." *Studies in Conflict & Terrorism* 33, no. 12 (2010): 1043–1078. Accessed May 22, 2011. http://dx.doi.org/10.1080/1057610X.2010.523860.

Hafez, Mohammed M. “Martyrdom Mythology in Iraq: How Jihadists Frame Suicide Terrorism in Videos and Biographies.” *Terrorism and Political Violence* 19, no. 95 (2007): 97–98.

Hahn, Gordon. “The Jihadi Insurgency and the Russian Counterinsurgency in the North Caucasus.” *Post-Soviet Affairs* 24, no. 1 (January–March 2008): 1–39. Accessed April 20, 2011. http://bellwether.metapress.com/content/90vpnp3464h5243h/fulltext.pdf.

Hammerli, August, Regula Gattiker, and Reto Weyermann. “Conflict and Cooperation in an Actor’s Network of Chechnya Based on Event Data.” *Journal of Conflict Resolution* 50, no. 2 (April 2006): 159–175. Accessed March 8, 2011. http://www.jstor.org/stable/276638482.

Hammes, Colonel Thomas X. *The Sling and the Stone: On War in the 21st Century*. St. Paul, MN: Zenith Press, 2004.

———. “Information Operations in 4GW.” In *Global Insurgency and the Future of Armed Conflict*, edited by Terry Terriff, Aaron Karp, and Regina Karp, 203. New York: Routledge, 2008.

———. “Rethinking the Principles of War: The Future of Warfare.” In *Rethinking the Principles of Wa*r, edited by Anthony McIvor. Annapolis, MD: Naval Institute Press, 20056.

———. “Why Study Small Wars?” *Small Wars Journal* 1 (April 2005).

———. *The Sling and the Stone: On War in the 21st Century*. St. Paul, MN: Zenith Press, 2004.

Hamzeh, Ahmad Nizar. *In the Path of Hizbullah*. Syracuse, NY: Syracuse University Press, 2004.

Hanna, David P. *Designing Organizations for High Performance*. New York: Addison-Wesley Publishing, Co., 1988.

Harb, Mona, and Reinoud Leenders. “Know Thy Enemy: Hizbullah, ‘Terrorism’ and the Politics of Perception.” *Third World Quarterly* 26, no. 1 (2005): 173–197. Accessed April 29, 2011. http://www.jstor.org/stable/3993770.

Harik, Judith Palmer. *Hezbollah: The Changing Face of Terrorism*. New York: I.B. Taurus & Co. Ltd., 2004.

Harmon, Christopher C. “Vulnerabilities of Terror Groups.” *Lexington Institute*, March 2007. Accessed December 11, 2010. www.lexingtoninstitute.org.

Hart, B.H. Liddell. *Lawrence of Arabia*. New York: DeCapo Press, 1989.

———. *Strategy*. New York: Frederick A. Praeger Publishers, 1954.

———. *Thoughts on War*. London: Farber and Farber, 1944.

Hartman, LTC William J. "Exploitation Tactics: A Doctrine for the 21st Century." Monograph, School of Advanced Military Studies. Fort Leavenworth, KS: United States Army Command and General Staff College, 2008.

Hashim, Ahmed S. *Insurgency & Counter-insurgency in Iraq*. Ithaca, NY: Cornell University Press, 2006.

Heffner, Michael, and Nawaz Sharif. "Knowledge Fusion for Technological Innovation in Organizations." *Journal of Knowledge Management* 12, no. 2 (2008): 79–93.

Helmer, Daniel I. *Flipside of the COIN: Israel's Lebanese Incursion Between 1982–2000*. Fort Leavenworth, KS: Combat Studies Institute Press, 2006.

———. "Not Quite Counterinsurgency: A Cautionary Tale for U.S. Forces Based on Israel's Operation Change of Direction." *Armor* CXVI, no. 1 (January–February 2007). Accessed May 4, 2011. https://www.knox.army.mil/center/armormag/currentissues/2007/Jf07/1Helmer07c.pdf.

Henriksen, Thomas H. *The Israeli Approach to Irregular Warfare and Implications for the United States*. JSOU Report 07-3. Hurlburt Field, FL: The Joint Special Operations University Press, 2007.

Henze, Paul B. *Islam in the North Caucasus*. Santa Monica: CA, RAND, 1995.

———. *Russia and the Caucasus*. Santa Monica, CA: RAND, 1996.

———. *The North Caucusus: Russia's Long Struggle to Subdue the Circassians*. Santa Monica: RAND, 1990.

Himelfarb, Joel. "Hezbollah's Deadly Record." *The Washington Times*, March 16, 2005. Quoted in Matt Matthews, *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War*. Fort Leavenworth, KS: Combat Studies Institute Press, 2008.

Hoffman, Bruce, and Jennifer M. Taw. *Defense Policy and Low-Intensity Conflict: The Development of Britain's 'Small Wars' Doctrine During the 1950s*. Santa Monica, CA: RAND, 164).

Hoffman, Bruce. "Defining Terrorism." In *Terrorism and Counter-Terrorism: Understanding the New Security Environment*, edited by Russell D. Howard and Reid L. Sawyer. 22. Guilford, CT: McGraw-Hill, 2003.

———. “Insurgency and Counterinsurgency in Iraq.” *Studies in Conflict and Terrorism* 29, no. 11 (2006): 103–121. Accessed November 20, 2010. http://dx.doi.org/10.1080/10576100500522173.

———. *Inside Terrorism*. New York: Columbia University Press, 2006.

Hoffman, Frank G. “Mind Maneuvers.” *Armed Forces Journal* (April 2007). Accessed April 21, 2011. http://www.armedforcesjournal.com/2007/04/2550166/.

———. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies, 2007.

IntelCenter. *Al-Qaeda Targeting Guidance*, vol. 1.0, Thursday, April 1, 2004. Alexandria, VA: Tempest Publishing, 2004.

International Crisis Group. “Terrorism in Indonesia: Noordin’s Networks.” *Asia Report #114*, (Brussels, Belgium: International Crisis Group, 2006. Accessed February 3, 2011. http://www.crisisgroup.org/en/regions/asia/south-east-asia/indonesia/114-terrorism-in-indonesia-noordins-networks.aspx.

“Israel Intelligence in the Second Lebanon War.” *Jane’s Intelligence Digest*, September 15, 2006. Accessed April 28, 2011. http://jiwk.janes.com/MicroSites/index.jsp?site=jiwk&pageindex=doc_view&K2DocKey=/content1/janesdata/mags/jiwk/history/jid2006/jid70085.htm.

“It Takes a Network.” Meeting of the International Counter-Terrorism Academic Community, ICT Newsletter, Spring 2010. Accessed October 11, 2010. http://www.ict.org.il/LinkClick.aspx?fileticket=Q-dvDwLODkc%3d&tabid=68Iskhanov, COL Husein. Interview. *Small Wars Journal* (June 1999). Accessed February 8, 2011. www.smallwarsjournal.com.

Janssens, Maddy, and Jeanne M. Brett. “Cultural Intelligence in Global Teams: A Fusion Model of Collaboration.” *Group & Organizational Management* 31, no. l (February 1, 2006): 124–153.

John P. Sullivan, and Adam Elkus, “Strategy and Insurgency: An Evolution in Thinking?” Accessed February 9, 2011. http://www.opendemocracy.net.

John R. Ballard, *Fighting for Fallujah: A New Dawn for Iraq*. Westport, CT: Praeger Security International, 2006.

Johnson, David T. Assistant Secretary, U.S. State Department. “Fighting Networks with Networks: Partnership and Shared Responsibility on Combating Transnational Crime.” Keynote Speech, Trans-Pacific Symposium on Dismantling Illicit Networks, Honolulu, Hawaii, November 10, 2009. Accessed December 13, 2010. http://www.state.gov/p/inl/rls/rm/131805.htm.

Jones, Calvert W. “Exploiting Structural Weaknesses in Terrorist Networks: Information Blitzkrieg and Related Strategies.” In *Ideas as Weapons: Influence and Perception in Modern Warfare*, edited by G. J. David Jr. and T. R. McKeldin, III, 7. Dulles, VA: Potomac Books, Inc., 2009.

Kahn, David. “A Historical Theory of Intelligence.” In *Intelligence Theory: Key Questions and Debates*, edited by Peter Gill, Steven Marrin, and Mark Pythian, 5–10. New York: Routledge, 2009.

Kalb, Marvin, and Carol Saivetz. “The Israeli-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict.” Paper prepared for the U.S.-Islamic World Forum on February 18, 2007. Accessed April 16, 2011). http://www.brookings.edu/~/media/Files/events/2007/0217islamic%20world/2007islamforum_israel%20hezb%20war.pdf.

Karasik, Theodore. “Chechen Clan Tactics and Russian Warfare.” March 15, 2000. Accessed April 8, 2011. http://www.cacianalyst.org/?q=353.

Katz, Yaakov. “The War in Numbers.” *Jerusalem Post*, August 6, 2006. Accessed April 28, 2011. http://www.jpost.com/Israel/Article.aspx?id=30756.

Katzenbach, Jon, and Douglas Smith. *The Wisdom of Teams: Creating the High Performance Organization*. Boston: Harvard Business School Press, 1993.

Katzman, Kenneth. “Al-Qaeda in Iraq: Assessment and Outside Links.” *CRS Report RL32217*, August 15, 2008. Accessed March 8, 2011. http://www.fas.org/sgp/crs/terror/RL32217.

Keegan, John. *The Iraq War*. New York: Alfred A. Knopf, 2004.

Kelley, MG John F. Quoted in Gary W. Montgomery and Timothy S. McWilliams, *Al-Anbar Awakening, Volume II: Iraqi Perspectives, From Insurgency to Counterinsurgency in Iraq, 2004–2009*. Washington, DC: Government Printing Office, 2009. Accessed May 15, 2011. http://smallwarsjournal.com/documents/anbar awakening2.pdf.

Kenney, Michael. *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation*. University Park, PA: Pennsylvania State University Press, 2007.

Kilcullen, David. “Build It and They Will Come.”—Use of Parallel Networks to Defeat Adversary Networks.” In *Proceedings on Strategy, Analysis, and Technology*, edited by Ronald R. Luman, Unrestricted Warfare Symposium, 2006. Accessed May 23, 2011. http://www.jhuapl.edu/ourwork/nsa/projects.asp.

———. “Counter-Insurgency Redux.” *Survival* 48, no. 4 (2006): 111–130.

———. *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*. New York: Oxford University Press, 2009.

Kimmage, Daniel, and Kathleen Ridolfo. “Iraqi Insurgent Media: The War of Ideas and Images.” *Central European Journal* 1, no. 2 (November 2007): 7–89. Accessed June 5, 2011. http://kms2.isn.ethz.ch/serviceengine/File/RESSpecNet/99882/ipublicationdocument_singledocument/BEB76AD2-D23D-4E2A-9A1D-D15102.

Kiras, James D. *Special Operations and Strategy*. New York: Routledge, 2006.

Kitson, Frank. *Low-Intensity Operations: Subversion, Insurgency, Peacekeeping*. London: Faber & Faber, 1971.

Kitson, MAJ Frank. *Gangs and Counter-Gangs*. London: Barrie and Rockliff, 1960.

Knezys, Stasys, and Romanas Sedlickas. *The War in Chechnya*. College Station, TX: Texas A&M University Press, 1999.

Kohlman, Evan F. “State of the Sunni Insurgency in Iraq.” Accessed July 15, 2010. http://www.nefafoundation.org/index.cfm?pageID=24.

Komer, Robert W. *Bureaucracy Does Its Thing: Institutional Constraints on U.S.—GVN Performance in Vietnam*. Santa Monica, CA: RAND, 1972.

Konovalov, Sergei. “Kontrterroristicheskaya operatsiya: Voennye i militsiya podelili Chechnyu na zony otvetstvennosti.” *Kommersant*, January 19, 2004. Cited in Mark Kramer, “Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus: The Military Dimension of the Russian-Chechen Conflict.” *Europe-Asia Studies* 57, no. 2 (March 2005): 209–290. Accessed October 14, 2010. http://dx.doi.org/10.1080/09668130500051833.

Kramer, Mark. “Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus: The Military Dimension of the Russian-Chechen Conflict.” *Europe-Asia Studies* 57, no. 2 (March 2005): 209–290. Accessed October 14, 2010. http://dx.doi.org/10.1080/09668130500051833.

———. “The Perils of Counterinsurgency: Russia’s War in Chechnya.” *International Security* 29, no. 3 (Winter 2004/2005): 5–63. Accessed October 9, 2011. http://belfercenter.ksg.harvard.edu./files/kramer.pdf.

Krebs, Valdis. “Mapping Networks of Terrorist Cells.” *Connections* 24, no. 3. Accessed September 19, 2010. http://www.sfu.ca/~insna/Connections-Web/Volume24-3/Valdis.Krebs.web.pdf.

Kuhn, Thomas S. *The Structure of Scientific Revolutions*. Chicago: University of Chicago Press, 1962.

Kydd, Andrew H., and Barbara F. Walter. “Strategies of Terrorism.” *International Security* 31, no. 1 (2006): 49–80.

Lamb, Christopher J., and Evan Musing. “Secret Weapon: High-Value Target Teams as an Organizational Innovation.” *Institute for National Strategic Studies Strategic Perspectives* no. 4 (2011): 33.

Lang, Qiao, and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999. Accessed February 12, 2011. http://www.cryptome.org/cuw.zip.

Laqueur, Walter. *The Guerrilla Reader*. New York, 1977.

Latimer, Jon. *Deception in War*. New York: Overlook Press, 2001.

Lawrence, Paul R., and Jay W. Lorsch. *Organization and Environment, Managing Differentiation and Integration*. Boston: Graduate School of Business Administration, Harvard University, 1967.

Leenders, Reinoud. “How the Rebel Regained His Cause Hizbullah and The Sixth Arab-Israeli War.” In *The Sixth War: Israel’s Invasion of Lebanon, The MIT Journal of Middle East Studies* 6 (Summer 2006). Accessed April 20, 2011. http://web.mit.edu/cis/www/mitejmes/.

Lesser, Ian O. “Countering the New Terrorism: Implications for Strategy.” In *Countering the New Terrorism*, edited by Ian O. Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt, and Michele Zanini, 118. Santa Monica, CA: RAND, 1999.

Lesser, Ian O., Bruce Hoffman, John Arquilla, David Ronfeldt, and Michele Zanini. *Countering the New Terrorism*. Santa Monica, CA: RAND, 1999.

Lezvina, Valentina. “Exercises in the Caucasus.” (in Russian), *Kommersant-Daily*, July 21, 1998, FBIS-UMA-98-217. Cited in Olga Oliker, *Russia’s Chechen Wars 1994–2000: Lessons Learned from Urban Combat*. Santa Monica, CA: RAND, 2001.

Lia, Brynjar. *Architect of Global Jihad: The Life of Al-Qaeda Strategist Abu Mus’ab al-Suri*. Cambridge University Press India, 2008.

Libicki, Martin. *What is Information Warfare?* Washington, DC: National Defense University, U.S. Government Printing Office, 1995.

Lind, William S. “Understanding Fourth Generation Warfare.” *Military Review* 84, no. 5 (2004): 12–16.

Long, Austin. *Doctrine of Eternal Recurrence: The U.S. Military and Counterinsurgency Doctrine, 1960–1970 and 2003–2006*. Santa Monica, CA: RAND, 2008.

Luttwak, Edward N. “Notes on Low-Intensity Warfare.” *Parameters* 13 (December 1983): 335–337.

Lynch, T. F. III. “Conceptual and Operational Challenges of COIN: Executive Summary.” *Joint Forces Quarterly* 60, no. 1 (2011), National Defense University Press. Accessed February 8, 2011. http://www.ndupress.ndu.edu.

Machiavelli, Niccoló. *The Prince*. Translated by George Bull. London: Penguin Books, 1999.

Mackey, Sandra. *The Reckoning: Iraq and the Legacy of Saddam Hussein*. New York: W.W. Norton & Company, 2003.

Makovsky, David, and Jefferey White. *Lessons and Implications of the Israel-Hizballah War,* Policy Focus #60. Washington, DC: Washington Institute for Near East Policy, 2006.

Marcos, Subcomandante Insurgente. *Our Word Is Our Weapon: Selected Writings.* Edited by Juana Ponce de Leon. New York: Seven Stories Press, 2002.

Marr, Phebe. *The Modern History of Iraq*. Boulder, CO: Westview Press, 1985.

Marrero, LTC Abe F. “The Tactics of Operation CAST LEAD.” In *Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD,* edited by LTC Scott C. Farquhar, 84. Fort Leavenworth, KS: Combat Studies Institute Press, 2009.

Marshall, S. L. A. *Men Against Fire: The Problem of Battle Command in Future Wars*. Alexandria, VA: Byrrd Enterprises, Inc., 1961.

Matthews, Matt. “Hard Lessons Learned.” In *Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD,* edited by LTC Scott C. Farquhar, 23. Fort Leavenworth, KS: Combat Studies Institute Press, 2009.

———. *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War*. Fort Leavenworth, KS: Combat Studies Institute Press, 2008.

McChrystal, Stanley A. “It Takes a Network: The New Frontline of Modern Warfare.” *Foreign Policy*, March/April 2011. Accessed February 24, 2011. http://www.foreignpolicy.com/articles/2011/02/22/it_takes_a_network.

———. “Listen, Learn, … then Lead.” Presented at the TED Conference, March 2011. Accessed April 13, 2011. http://www.ted.com/talks/stanley_mcchrystal.html.

McClure, Sean. “The Lost Caravan: The Rise and Fall of Al Qaeda in Iraq, 2003–2007.” Master’s thesis, Monterey, CA: Naval Postgraduate School, 2009.

McCormick, Gordon. “Diamond Insurgent/COIN Model.” Depicted in Eric P. Wendt, “Strategic Counterinsurgency Modeling.” *Special Warfare* 18, no. 2 (September 2005): 5–6.

McGuire, MAJ Michael J. *Modeling the Effect of Direct Action Operations on an Insurgent Population*. Newport, RI: Naval War College, 2008.

McMaster, H. R. “On War: Lessons to be Learned.” *Survival: Global Politics and Strategy* 50, no. 1 (2008): 21. Accessed May 6, 2011. http://dx.doi.org/10.1080/00396330801899439.

McNeive, LTC James. “Frustration.” In *Ideas As Weapons: Influence and Perception in Modern Warfare*, edited by G. J. David Jr. and T. R. McKeldin III, 357–361. Washington, DC: Potomac Books, 2009.

McRaven, William H. *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice*. Novato, CA: Presidio Press, 1995.

McShane, Steven L., and Mary Ann Von Glinow. *Organizational Behavior*. Boston: McGraw-Hill Irwin, 2007.

Metz, LTG Thomas F. “Massing Effects in the Information Domain: A Case Study in Aggressive Information Operations.” In *Ideas As Weapons: Influence and Perception in Modern Warfare*, edited by G. J. David Jr. and T. R. McKeldin III, 266. Washington, DC: Potomac Books, 2009.

Milgram, Stanley. “The Small World Problem.” *Psychology Today* (1967): 60–67.

Mintzberg, Henry. “Organizational Design, Fashion or Fit?” *Harvard Business Review* (January–February 1981, reprint 81106), 5.

Mishal, Shaul, and Maoz Rosenthal. “Al-Qaeda as a Dune Organization: Toward a Typology of Islamic Terrorist Organizations.” *Studies in Conflict & Terrorism* 28, no. 4 (2005): 275–293. Accessed May 22, 2011. http://dx.doi.org/10.1080/10576100590950165.

Montgomery, Gary W., and Timothy S. McWilliams. *Al-Anbar Awakening, Volume II: Iraqi Perspectives, From Insurgency to Counterinsurgency in Iraq, 2004–2009*. Washington, DC: Government Printing Office, 2009.

Moore, MAJ Sharon Tosi. “2006 Lebanon War: An Operational Analysis.” In *Joint Center for Operational Analysis Journal* 10, no. 1 (2007): 19.

Morselli, Carlo, and Katia Petit. “Law-Enforcement Disruption of a Drug Importation Network.” *Global Crime* 8, no. 2 (May 2007): 17.

Mukasey, Michael B. “How a Bagram Detainee Foiled the Euro Terror Plot.” *Wall Street Journal*, October 8, 2010, 19.

Mukhin, Vladimir. “V Chechne voyuyut glavnym obrazom spetspodrazdeleniya.” *Armeiskii sbornik*, July 7, 2003, 32–33. Cited in Mark Kramer, “Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus: The Military Dimension of the Russian-Chechen Conflict.” *Europe-Asia Studies* 57, no. 2 (March 2005): 209–290. Accessed October 14, 2010. http://dx.doi.org/10.1080/09668130500051833.

Multi-National Coalition-Iraq SIGACTS Reports, 2007–2009. Accessed May 20, 2011. http://www.globalsecurity.org/military/ops/iraq_sigacts.htm.

Multi-National Force-Iraq. “Fusion Cells to Help Locate Terrorists.” *Combined Press Information Center*. December 14, 2006. Accessed May 18, 2011. http://www.usf-iraq.com/?option=com_content&task=view&id=8093&Itemid=21.

———. “Iraqi Fusion Cells Bring U.S., Iraqi intelligence-Gathering to New Heights.” July 23, 2009. Accessed May 18, 2011. http://www.globalsecurity.org/military/library/news/2009/07/mil-090723-mnfi02.htm.

Murphy, Paul. *The Wolves of Islam*. Washington, DC: Brassey’s Inc., 2004.

Nagl, John. “Strategic Innovation: Integrating National Power to Win in Iraq.” In *Ideas as Weapons: Influence and Perception in Modern Warfare*, edited by G. J. David Jr. and T. R. McKeldin, III, 95. Dulles, VA: Potomac Books, Inc., 2009.

Nagl, John. *Learning to Eat Soup With a Knife: Counterinsurgency Lessons from Malaya and Vietnam*. Westport, CT: Praeger Publishers, 2002.

Najem, Tom P. “Palestinian-Israeli Conflict and South Lebanon.” *Economic and Political Weekly* 35, no. 46 (November 11–17, 2000): 4006–4009. Accessed April 29, 2011. (http://www.jstor.org/stable/4409949.

Nance, Malcolm W. *The Terrorists of Iraq*. Internet Publishing, www.booksurge.com, 2007.

Napoleoni, Loretta. *Insurgent Iraq: Al-Zarqawi and the New Generation*. New York: Seven Stories Press, 2005.

Nasrallah, Hassan. “Interview with New TV.” In *Voice of Hezbollah: The Statements of Sayyed Hassan Nasrallah*, edited by Nicholas Noe, 390–391. Princeton, NJ: Princeton University Press, 2007.

———. “We Will Consider Any Hand that Tries to Seize Our Weapons As An Israeli Hand.” In *Voice of Hezbollah: The Statements of Sayyed Hassan Nasrallah*, edited by Nicholas Noe, 338. Princeton, NJ: Princeton University Press, 2007.

Nekrich, Aleksander M. *The Punished Peoples*. Translated by George Saunders. New York: W.W. Norton and Co., 1978.

Nemeth, William J. “Future War and Chechnya: A Case for Hybrid Warfare.” Master’s thesis, Monterey, CA: Naval Postgraduate School, 2002.

Newman, Mark, Albert-László Barabási, and Duncan J. Watts, ed. *The Structure and Dynamics of Networks.* Princeton, NJ: Princeton University Press, 2006.

Ney, Virgil. *Notes on Guerrilla War: Principles and Practices*. Washington, DC: Command Publications, 1961.

Norton, Augustus Richard. *Amal and the Shi’a: Struggle for the Soul of Lebanon.* Austin, TX: University of Texas Press, 1987.

———. *Hezbollah*. Princeton, NJ: Princeton University Press, 2007.

Oliker, Olga. *Russia’s Chechen Wars 1994–2000: Lessons Learned from Urban Combat*. Santa Monica, CA: RAND, 2001.

Opall-Rome Barbara. “Israel May Disrupt Commercial Broadcasts.” *Defense News*, August 28, 2006. Accessed April 20, 2011. www.oss.net/dynamaster/file_archive/060831.

———. “Sensor to Shooter in 1 Minute.” *Defense News*, October 2, 2006.

Operational Implications of Effects-Based Operations (EBO). Joint Doctrine Series, no. 7. Fort Monroe, VA: Joint Warfighting Center, November 17, 2004.

Ottoman, Sharon. “Iraq: The Sunnis.” *Council of Foreign Relations*. Accessed April 18, 2011. http://www.cfr.org/iraq/iraq-sunnis/p7678.

Packer, George. “Knowing the Enemy: Can Social Scientists Redefine the ‘War on Terror?’” *The New Yorker*, December 18, 2006, 65–66. Accessed March 23, 2011. http://www.newyorker.com/archive/2006/12/18/061218fa_fact2.

Paget, Julian. *Counter-Insurgency Operations: Techniques of Guerrilla Warfare.* New York: Walker and. Company, 1967.

Partlow, Joshua. “For U.S. Unit in Baghdad, an Alliance of Last Resort.” *The Washington Post*, June 9, 2007, Section A.

Paul, Christopher, Colin P. Clarke, and Beth Gill. "Victory Has a Thousand Fathers: Evidences of Effective Approaches to Counterinsurgency, 1978–2008." *Small Wars Journal*, 8. Accessed February 25, 2011. http://www.smallwarsjournal.com.

Pescosolido, Bernice A., and Sharon Georgianna. "Durkheim, Suicide, and Religion: Toward a Network Theory of Suicide." *American Sociological Review* 54, no. 1 (1989): 33–48.

Pfeffer, Jeffrey. *Locations in the Communications Network*. Boston: Harvard Business School Press, 1994.

Phillips, Andrew. "How al-Qaeda Lost Iraq." *Australian Journal of International Affairs* 63, no. 1 (2009): 64–84.

Pollard, Neal A. "Globalization's Bastards: Illegitimate Non-State Actors in International Law." *Law Intensity Conflict & Law Enforcement* 12, no. 3 (2004). Accessed November 15, 2010. http://dx.doi.org/10.1080/0966284042000279009.

Posen, Barry. *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars*. Ithaca, New York: Cornell University Press, 1984.

Powell, Walter W. "Neither Market nor Hierarchy: Network Forms of Organization." *Research in Organizational Behavior* 12 (1990): 295–336.

Pratkanis, Anthony R. "Winning Hearts and Minds: A Social Influence Analysis." In *Information Strategy and Warfare: A Guide to Theory and Practice*, edited by John Arquilla and Douglas A. Borer, 56–80. New York: Routledge, 2007.

Proceedings of the Unrestricted Warfare Symposium. Published yearly 2006–2009. Accessed April 20, 2011. http://www.jhuapl.edu/ourwork/nsa/projects.asp.

Qassem, Sheikh Naim. *Hizbullah: The Story From Within*. Translated by Dalia Khalil. London, Saqi, 2005.

Raab, Jorge, and H. Brinton Milward. "Dark Networks as Problems." *Journal of Public Administration Research and Theory* (October 2003): 417.

Raphaeli, Nimrod. "The Sheikh of the Slaughters: Abu Musa'b Al-Zarqawi and the Al-Qaeda Connection." *Middle East Research Institute.* Accessed March 9, 2011. http://www.memri.org/report/en/0/0/0/0/0/0/1406.htm.

Rechkalov, Vadim. "'Budut lokal'nye stychki s zhertvami do 100 chelovek, a voiny ne budet': Bandformirovaniya Severnogo Kavkaza osvaivayut novuyu taktiku." *Izvestiya*, August 2, 2004. Cited by Mark Kramer, "Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus: The Military Dimension of the Russian-Chechen Conflict." *Europe-Asia Studies* 57, no. 2 (March 2005): 209–290. Accessed October 14, 2010. http://dx.doi.org/10.1080/09668130500051833.

Reid-Daly, LTC Ronald F. *Pamwe Chete: The Legend of the Selous Scouts*. Weltevreden Park, South Africa: Covos-Day, 2000.

Richards, COL Chet (Ret.), LTC Greg Wilcox (Ret.), and COL G. I. Wilson (Ret.). "America in Peril: Fourth Generation Warfare in the Twenty-First Century." In *Global Insurgency and the Future of Armed Conflict*, edited by Terry Terriff, Aaron Karp, and Regina Karp, 122, 127. New York: Routledge, 2008.

Ricks, Thomas. "Counterinsurgency: The Brutal but Effective Russian Approach." *Foreign Policy*, September 17, 2009. Accessed May 23, 2011. http://ricks.foreignpolicy.com/posts/2009/09/17/counterinsurgency_the_brutal_but_effective_russian_approach.

———. *The Gamble: General David Petraeus and the American Military Adventure in Iraq, 2006–2008*. New York: Penguin Press, 2009.

Rid, Thomas, and Marc Hecker. *War 2.0: Irregular Warfare in the Information Age*. Westport, CT: Praeger Security International, 2009.

Riedel, Bruce. *The Search for Al-Qaeda: It's Leadership, Ideology, and Future*. Washington, DC: Brookings Institution Press, 2008.

Robb, John. *Brave New War*. Hoboken, NJ: John Wiley & Sons, 2007.

Robinson, Glenn. "Identity Politics and the War in Iraq." In *The Three Circles of War: Understanding the Dynamics of Conflict in Iraq*, edited by Heather S. Gregg, Hy S. Rothstein, and John Arquilla, 13. Washington, DC: Potomac Books, 2010.

Robinson, Linda. *Masters of Chaos: The Secret History of the Special Forces*. New York: Public Affairs, 2004.

Rodriguez, Jose A. "The March 11th Terrorist Network: In Its Weakness Lies Its Strength." Presented at Sunbelt XXV: International Sunbelt Social Network Conference, February 16–21, 2005, Redondo Beach, CA.

Roggio, Bill. "Al-Qaeda in Iraq's Security Minister Captured in Anbar." *The Long War Journal*, December 1, 2010. Accessed December 7, 2010. http://www.longwarjournal.org/archives/2008/03/coalition_targets_al.php.

———. “Coalition Targets Al-Qaeda in the Iraqi North.” *The Long War Journal*, March 5, 2008. Accessed November 29, 2010. http://www.longwarjournal.org/archives/2008/03/coalition_targets_al.php.

Rollins, John. *Al Qaeda and Affiliates: Historical Perspectives, Global Presence, and Implications for U.S. Policy*, R41047. Washington, DC: U.S. Congressional Research Service, February 5, 2010.

Ronfeldt, David, and John Arquilla. “Emergence and Influence of the Zapatista Social Netwar.” In *Network and Netwars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and David F. Ronfeldt. 190. Santa Monica, CA: RAND, 2001.

Ronfeldt, David. “Al-Qaeda and its Affiliates: A Global Tribe Waging Segmental Warfare.” In *Information Strategy and Warfare: A Guide to Theory and Practice*, edited by John Arquilla and Douglas A. Borer, 1–15, 35. New York: Routledge, 2007.

Rosenburg, Steve. “Chechen Warlord Doku Umarov Admits Moscow Airport Bomb.” *BBC News*, February 8, 2011. Accessed April 11, 2011. http://www.bbc.co.uk/news/world-europe-12388681.

Roston, Clyde. “Terrorist to Techno-Guerrilla: The Changing Face of Asymmetric Warfare.” *Joint Center for Operational Analysis Journal* 10, no. 1 (December 2007): 45.

Roth, Kenneth. “The Wrong Way to Combat Terrorism.” *The Brown Journal of World Affairs* (Summer/Fall 2007): 116.

Sageman,Marc. *Understanding Terror Networks*. Philadelphia, PA: University of Pennsylvania Press, 2004.

Sankari, Jamal. *Fadallah: The Making of a Radical Shi’ite Leader*. London: Sadi, 2005.

Sarwary, Bilal. “Shift in Taliban Tactics Alarms Afghanistan Government. May 29, 2011, *BBC News South Asia*. Accessed May 28, 2011. http://www.bbc.co.uk/news/world-south-asia-13589764.

Sayigh, Yezid. “Israel’s Military Performance in Lebanon, June 1982.” *Journal of Palestine Studies* 13, no. 1 (1983): 24–65. Accessed April 29, 2011. http://www.jstor.org/stable/2536925.

Scales, Robert H. *Certain Victory: The U.S. Army in the Gulf War*. Washington, DC: Brassey’s, 1994.

Schanzer, Jonathan, and Dennis Ross. *Al-Qaeda's Armies: Middle East Affiliate Groups & the Next Generation of Terror*. Washington, DC: Washington Institute for Near East Policy, 2005.

Schroeder, Michael J. "Intelligence Capacities of the U.S. Military in the Sandino Rebellion, Las Segovias, Nicaragua, 1927–1932: Successes, Failures, Lessons." Accessed December 3, 2010. http://sandinorebellion.com/mjs/mjs-intel.htm.

Security Report on Al-Zarqawi, Ansar al-Sunnah Groups. From "Al-Zarqawi Was the Mastermind of the Attack on Dr. Barham." Published by *Awena*, February 28, 2006.

Seely, Robert. *Russo-Chechen Conflict 1800–2000: A Deadly Embrace*. London: Frank Cass, 2001.

Shachtman, Noah. "Some of Her Best Friends Are Terrorists." *WIRED*, October 23, 2007. Accessed May 20, 2011. http://www.wired.com/dangerroom/2007/10/some-of-her-bes/.

Shapira, Shimon. "The Origins of Hezbollah." *The Jerusalem Quarterly* 46 (1988): 115–130.

Sheehan, Ivan Sascha. *When Terrorism and Counterterrorism Clash*. Youngstown, NY: Cambria Press, 2007.

Shultz, Richard H., and Andrea J. Dew. *Insurgents, Terrorists, and Militias: The Warriors of Contemporary Combat*. New York: Columbia University Press, 2006.

Shy, John, and Thomas Collier. "Revolutionary War." In *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, edited by Peter Paret, 821. Princeton, NJ: Princeton University Press, 1986.

SIGACTS Chart. Accessed May 20, 2011. http://www.globalsecurity.org/military/ops/iraq_sigacts.htm.

Simmel, Georg. "The Secret and the Secret Society." In *The Sociology of Georg Simmel*, edited and translated by Kurt Wolff. New York: Free Press, 1950.

Simpkin, Richard E. *Race to the Swift: Thoughts on Twenty-First Century Warfare*. London: Brassey's, Inc., 2000.

Sinno, Abdulkader H. *Organizations at War in Afghanistan and Beyond*. Cornell University Press, 2007.

Smith, MAJ Neil, and COL Sean MacFarland. "Anbar Awakens: The Tipping Point." *Military Review* 88, no. 2 (March/April 2008): 41–52.

Snyder, LTC Michael D. “Information Strategies Against a Hybrid Threat.” In *Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD*, edited by LTC Scott C. Farquhar, 104. Fort Leavenworth, KS: Combat Studies Institute Press, 2009.

Sobelman, Daniel. *New Rules of the Game: Israel and Hizballah after the Withdrawal from Lebanon*. Tel Aviv: Jaffee Center for Strategic Studies, Tel Aviv University, 2004.

Spulak, Robert G. Jr., and Jessica Glicken Turnley. “Theoretical Perspectives of Terrorist Enemies as Networks.” *Joint Special Operations University Report 05-03*. Hurlburt Field, FL: Joint Special Operations University Press, 2005.

Stanton, Doug. *Horse Soldiers*. New York: Scribner, 2009.

Sterling, Claire. *The Terror Network: The Secret War of International Terrorism*. New York: Holt, Rinehart, and Winston, 1981.

Stork, Joe, and Jim Paul. “The War in Lebanon.” From *MERIP Reports, No. 108/109, The Lebanon War*. Middle East Research and Information Project, September–October 1982. Accessed April 29, 2011. http://www.jstor.org/stable/3012233.

Stroumpos, LTC George J. “Clouding the Issue: Intelligence Collection, Analysis, and Dissemination during Operation Iraqi Freedom.” In *Ideas As Weapons: Influence and Perception in Modern Warfare*, edited by G. J. David Jr. and T. R. McKeldin III, 251. Washington, DC: Potomac Books, 2009.

Sunderland, Riley. *Antiguerrilla Intelligence in Malaya, 1948–1960*. Santa Monica, CA: RAND Corporation, 1964.

Taber, Robert. *War of the Flea: The Classic Study of Guerrilla Warfare*. Washington, DC: Potomac Books, 2002.

Teslick, Lee Hudson. “Profile: Abu Musab al-Zarqawi.” *Council on Foreign Relations*. Accessed May 15, 2011. http://cfr.org/publication/9866/.

Thomas, Tim L. “A Tale of Two Theaters: Russian Actions in Chechnya in 1994 and 1999.” *Analysis of Current Events* 12, no. 5–6 (2000): 2. Accessed October 9, 2011. http://fmso.leavenworth.army.mil/documents/chechtale.htm.

Thompson, Sir Robert. *Defeating Communist Insurgency: The Lessons of Malaya and Vietnam*. New York: Praeger Publishers, 1966.

Todd, Lin, W. Patrick Lang, Jr., Colonel, U.S. Army (Retired), R. Alan King, Andrea V. Jackson, Montgomery McFate, Ahmed S. Hashim, and Jeremy S. Harrington. *Iraq Tribal Study—Al Anbar Governorate: The Albu Fahd Tribe, the Albu Mahal Tribe, and the Albu Issa Tribe*. Arlington, VA: Global Resources Group, 2006. Accessed May 16, 2011. http://turcopolier.typepad.com/the_athenaeum/files/iraq_tribal_study_070907.pdf.

Trenin, Dimitri V., and Aleksei V. Malashenko. *Russia's Relentless Frontier: The Chechnya Factor in Post-Soviet Russia*. Washington, DC: Carnegie Endowment for International Peace, 2008.

Treverton, Gregory F. *Intelligence for an Age of Terror*. New York: Cambridge University Press, 2009.

Trinquier, Roger. *Modern Warfare: A French View of Counterinsurgency*. Translated by Daniel Lee. Westport, CT: Praeger Security International, 2006.

Tucker, David. "Terrorism, Networks and Strategy: Why the Conventional Wisdom is Wrong." *Homeland Security Affairs* 4, no. 2 (June 2008): 2, 4. Accessed October 19, 2010. http://www.hsaj.org/?article=4.2.5.

Turbiville, Graham H. Jr. "Hunting Leadership Targets in Counterinsurgency and Counterterrorist Operations." *Joint Special Operations University Report 07-6*. Hurlburt Field, FL: Joint Special Operations University Press, 2007.

Turnley, Jessica Glicken. "Implications for Network-Centric Warfare." *Joint Special Operations University Report 06-3*. Hurlburt Field, FL: Joint Special Operations University Press, 2006.

Tzu, Sun. *The Art of War*. Translated and edited by Samuel B. Griffith. London: Oxford University Press, 1971.

'Uthman. Nu'man ibn. Former Afghan jihadi. Interview in *Al-Hayat*. Cited in "Former Jihad Fighter in Afghanistan: Al-Zarqawi's Group Adopted the Worst Practices of the Algerian GIA: Their Brutal Actions Will Lead to their Isolation." Accessed May 18, 2011. http://www.memri.org/report/en/0/0/0/0/0/0/1256.html.

"U.S.: 2 of Al-Qaeda's Top Leaders Killed in Iraq." *CBS News*, April 19, 2010. Accessed April 29, 2010. http://www.cbsnews.com/stories/2010/04/19/world/main6410912.shtml.

U.S. Department of Defense. "Measuring Stability and Security in Iraq." September 2009. Cited in John Rollins. *Al Qaeda and Affiliates: Historical Perspectives, Global Presence, and Implications for U.S. Policy*, R41047. Washington, DC: U.S. Congressional Research Service, February 5, 2010.

———. Department of Defense Directive 3000.7, *Irregular Warfare*. Washington, DC: U.S. Government Printing Office, 2008.

———. Field Manual 3-0, *Operations*. Washington, DC: U.S. Government Printing Office, 2008.

———. Field Manual 3-24, *Counterinsurgency*. Washington, DC: U.S. Government Printing Office, 2006.

———. *Irregular Warfare Joint Operating Concept*, Version 1.0. Washington, DC: U.S. Joint Chiefs of Staff, January 2007.

———. *Irregular Warfare: Countering Irregular Threats Joint Operational Concept v.2.0*. Washington, DC: U.S. Government Printing Office, 2010.

———. Joint Chiefs of Staff. *The National Military Strategy of the United States*. February 8, 2011.

———. Joint Publication 1, *Doctrine for the Armed Forces of the United States*. Washington, DC: U.S. Government Printing Office.

———. Joint Publication 1-02, *Dictionary of Military and Associated Terms* (JP 1-02). U.S. Government Printing Office, 2009.

———. Joint Publication 3-0, *Joint Operations*. Washington, DC: U.S. Government Printing Office, 2010.

———. Joint Publication 3-05.01, *Joint Tactics, Techniques, and Procedures for Joint Special Operations Task Force Operations*. Washington, DC: U.S. Government Printing Office, 2007.

———. Joint Publication 3-26, *Counterterrorism*. Washington, DC: U.S. Government Printing Office, 2009.

U.S. Department of State. Office of the Coordinator for Counterterrorism. *Patterns of Global Terrorism*, 2003. Accessed February 8, 2011. http://www.state.gov/s/ct/rls/crt/2003/index.htm.

U.S. Joint Chiefs of Staff. *The National Military Strategy of the United States*, February 8, 2011.

U.S. Joint Forces Command. "Cross Functional Fusion Cells: Application of Tactical Fusion Cells at Higher Echelons." Concept White Paper V 1.5 (January 8, 2008).

U.S. Senate Armed Forces Committee on July 9, 2003. In Anthony Cordesman, *The Iraq War: Strategy, Tactics, and Military Lessons*, 3. Westport, CT: Praeger Publishers, 2003.

U.S. Senate Committee on Armed Services. *Current and Future Worldwide Threats to the National Security of the United States*, February 12, 2003.

University of Texas at Austin. University of Texas Libraries. Perry–Castañeda Library Map Collection. Chechenya (Chechen Republic) Maps. Accessed April 22, 2011. http://www.lib.utexas.edu/maps/chechen.html.

———. University of Texas Libraries. Perry–Castañeda Library Map Collection. Iraq Maps. Accessed May 24, 2011. http://www.lib.utexas.edu/maps/iraq.html.

———. University of Texas Libraries. Perry–Castañeda Library Map Collection. Lebanon Maps. Accessed May 12, 2011. http://www.lib.utexas.edu/maps/lebanon.html.

Urban, Mark. *Task Force Black: The Explosive True Story of the SAS and the Secret War in Iraq*. London: Little, Brown Publishing, 2010.

Vego, Milan N. "Increasing Doctrinal Wisdom." *Joint Force Quarterly* (April 1, 2009).

———. "Systems versus Classical Approach to Warfare." *Joint Forces Quarterly* no. 52 (1st Quarter 2009): 42.

Verton, Dan. *Black Ice: The Invisible Threat of Cyber-Terrorism*. New York: McGraw-Hill Osborne Media, 2003.

Volckmann, Russell W. Col. *We Remained*. New York: W.W. Norton Co., 1954.

Warrick, Joby, and Robin Wright. "U.S. Teams Weaken Insurgency in Iraq." *Washington Post*, September 6, 2008. Accessed January 13, 2011. http://www.washingtonpost.com/wp-dyn/content/article/2008/09/05/AR2008090503933.html.

Watts, Duncan, and Steve Strogatz. "Collective Dynamics of 'Small-World' Networks." *Nature* (1998): 440–442.

Weimann, Gabriel. *Terror on the Internet*. Washington, DC: United States Institute of Peace Press, 2006.

West, Bing. "Iraq and a Singular Information Failure." In *Ideas As Weapons: Influence and Perception in Modern Warfare*, edited by G. J. David Jr. and T. R. McKeldin III. Washington, DC: Potomac Books, 2009.

West, Francis J. *The Strongest Tribe: War, Politics, and the Endgame in Iraq*. New York: Random House, 2008.

The White House. "Interview of National Security Advisor by KXAS-TV, Dallas, TX." November 2003.

Winslow, Charles. *Lebanon: War and Politics in a Fragmented Society*. New York: Routledge, 1996.

Woodward, Bob. "Why Did Violence Plummet? It Wasn't Just the Surge." *Washington Post*, September 8, 2008. Accessed January 13, 2011. http://www.washingtonpost.com/wp-dyn/content/article/2008/09/07/AR2008090701847.html.

———. *The War Within: A Secret White House History 2006–2008*. New York: Simon & Schuster, 2008.

The World Factbook. Accessed May 12, 2011. https://www.cia.gov/library/publications/the-world-factbook/geos/le.html.

Ya'ari, Ehud. "Hizballah: 13 Principles of Warfare." *The Jerusalem Report*, March 21, 1996. Quoted in Daniel I. Helmer, *Flipside of the COIN: Israel's Lebanese Incursion Between 1982–2000*. Fort Leavenworth, KS: Combat Studies Institute Press, 2006.

Zanini, Michele, and Sean Edwards. "The Networking of Terrorism in the Information Age." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and David Ronfeldt, 30. Santa Monica, CA: RAND Corporation, 2001.

Zimmerman, LTC Frank H. "Attack, Attack, Attack, Information Operations." *IO Sphere*, Winter 2010, 10–17. Accessed May 23, 2011. http://usacac.army.mil/cac2/IPO/repository/iosphere.pdf.

Zurcher, Christopher. *The Post-Soviet Wars: Rebellion, Ethnic Conflict, and Nationhood in the Caucasus*. New York: New York University Press, 2007.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. John Arquilla
   Naval Postgraduate School
   Monterey, California

4. Dr. Michael Freeman
   Naval Postgraduate School
   Monterey, California

5. Dr. Gordon McCormick
   Naval Postgraduate School
   Monterey, California

6. Dr. Sean Everton
   Naval Postgraduate School
   Monterey, California

7. ASD/SOLIC
   Washington, D.C.

8. OSD/Office of Net Assessment
   Washington, D.C.

9. SOCOM J-7
   MacDill AFB, Florida

10. HQ USSOCOM Library
    MacDill AFB, Florida

11. Joint Special Operations University
    Hurlburt Field, Florida